Veeam Data Platform

100 premiers jours

Guide pratique d'intégration pour les administrateurs IT

Sommaire

1. Résumé

Veeam Data Platform est le socle de votre organisation pour assurer sa résilience face au ransomware et sa continuité opérationnelle. Ce guide est conçu pour aider les équipes informatiques à opérationnaliser et à faire évoluer leur environnement de manière structurée. Bien que nous utilisions l'expression « 100 premiers jours », il ne s'agit que d'une métaphore pour désigner une chronologie. Chaque organisation est différente et peut progresser à des rythmes différents, mais l'objectif reste le même : passer de la configuration initiale à un état plus sécurisé, résilient et prêt à la restauration. Elle est structurée autour de jalons pratiques et de résultats recommandés plutôt que d'exigences strictes d'implémentation, ce qui vous permet de vous concentrer sur les étapes les plus pertinentes pour votre environnement et votre édition.

2. À qui s'adresse ce guide ?

Ce guide s'adresse aux **administrateurs IT** qui déploient, configurent et mettent en œuvre la plateforme Veeam Data Platform. Ce guide part du principe que vous avez une bonne connaissance des infrastructures virtualisées (p. ex., VMware vSphere, Microsoft Hyper-V ou tout autre hyperviseur pris en charge par Veeam Backup & Replication) ainsi que des bases de l'administration de Windows Server. Aucune expertise Linux n'est requise.

Il sert également de référence partagée pour **les responsables informatiques** qui suivent le périmètre et les délais, les parties prenantes de la sécurité et de la conformité qui valident la posture de sécurité renforcée, ainsi que la direction ou les équipes d'achat, en définissant ce à quoi ressemble le succès du Jour 100.

3. Objectifs à atteindre au Jour 100

Au 100e jour, vous disposerez d'un environnement stable, durci et dont la récupération peut être vérifiée, qui réduit le risque de panne et permet une restauration rapide et fiable en toutes circonstances.

Chaque client doit être en mesure de confirmer que les points de contrôle suivants sont respectés :

- **Déployé :** Veeam Backup & Replication est en cours d'exécution, connecté et dimensionné pour respecter les fenêtres de sauvegarde.
- **Protégé :** les workloads prioritaires sont sauvegardés correctement selon un calendrier défini.
- **Renforcé :** l'inaltérabilité est en place localement et/ou hors site pour protéger contre les ransomwares.
- **Restauration vérifiable :** les tests de restauration sont terminés, documentés et alignés sur l'objectif de temps de restauration (RTO) et le délai optimal de reprise d'activité (RPO).
- **Opérationnalisé :** la supervision, l'alerte, le reporting et les runbooks de restauration sont en place et attribués.

4. Feuille de route en bref

Ce guide est structuré en quatre phases séquentielles, chacune visant les résultats du Jour 100 :

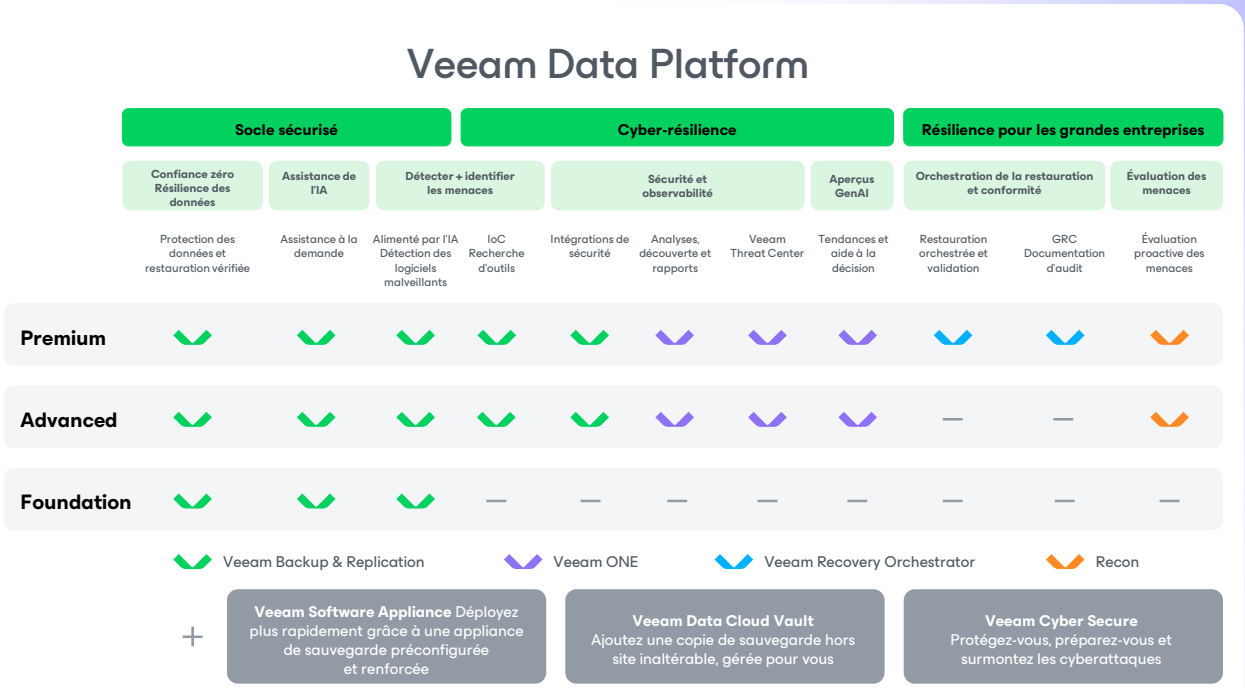
Phase	Nom	Chronologie	Objectif
PHASE 1	Foundation	Jours 1 à 14	Dimensionnez l'environnement, déployez l'appliance d'infrastructure Veeam (et l'appliance logicielle Veeam le cas échéant), exécutez les premières tâches de sauvegarde, préparez-vous à Veeam Recovery Orchestrator.
PHASE 2	Optimisation	Jours 15 à 45	Traitement prenant en charge les applications, tâches de copie des sauvegardes, niveau hors site de Veeam Data Cloud Vault et configuration de Veeam Recovery Orchestrator (Premium).
PHASE 3	Résilience des données et de l'activité	Jours 46 à 75	Comblez les lacunes de couverture, activez Recon, préparez-vous aux ransomwares, optimisez les réglages et élaborez des plans d'orchestration (Premium).
PHASE 4	Prouver la valeur	Jours 76 à 100	Tests de restauration orchestrés, rapports, architecture documentaire et hygiène continue.

Comment utiliser ce guide

- Suivez les jalons dans l'ordre. Sauter des étapes, en particulier la configuration du Scale-Out Backup Repository™ (SOBR) ou du Vault, avant que vos cibles et jobs locaux ne soient stables, crée des lacunes qui apparaissent généralement lors d'une restauration réelle.
- La chronologie est flexible. Les jours sont des lignes directrices, pas des délais stricts. Les petits environnements peuvent achever la phase 1 en moins d'une semaine. Les environnements plus complexes peuvent nécessiter plus de temps dans les phases ultérieures.
- Utilisez les points de décision. Lorsque des choix d'architecture se présentent (par exemple, chemin de déploiement ou stratégie de cible), faites une pause, alignez les parties prenantes et documentez votre décision avant de poursuivre.
- Passez ce qui ne s'applique pas, mais notez pourquoi. Si votre édition ne comprend pas Veeam ONE ou Veeam Recovery Orchestrator, ces jalons seront clairement identifiés. De même, les étapes concernant Veeam Software Appliance et Veeam Vault sont facultatives et pertinentes uniquement si ces modules font partie de votre déploiement.

Présentation de la Veeam Data Platform

Avant de nous lancer dans le déploiement et la façon de procéder, démarrons par un rapide aperçu de ce que comprend votre Veeam Data Platform. Veeam Data Platform est disponible en trois éditions, chacune s'appuyant sur la précédente :



Voir l'annexe pour les descriptions de tous les composants : « Annexe : Référence rapide. Principaux composants».

Prenez quelques instants pour confirmer votre édition.

Avant de poursuivre, confirmez votre édition et faites l'inventaire complet de ce qu'elle contient. En matière de protection des données, les fonctionnalités inutilisées ne sont pas seulement une valeur gaspillée — ce sont des lacunes qui attendent d'être exposées.

De plus, les modules suivants sont disponibles dans toutes les éditions :

- **Veeam Software Appliance :** une plateforme de déploiement pré-sécurisée, sans Windows, qui simplifie la mise en place de l'infrastructure et renforce la posture de sécurité. Aucune expertise Linux n'est requise.
- **Veeam Vault :** stockage de sauvegarde hors site inaltérable fourni en tant que service pour protéger vos données contre les ransomware et les suppressions accidentelles.
- **Veeam Agents :** les Veeam Agents sont des agents logiciels qui apportent une sauvegarde et une restauration au niveau image de qualité Veeam aux serveurs physiques, aux terminaux et aux plateformes de machines virtuelles (VM) non prises en charge, gérés de manière centralisée depuis la console Veeam Backup & Replication.

La voie vers la résilience commence ici.

Au cours des 100 prochains jours, vous passerez du déploiement à un environnement entièrement renforcé et récupérable de façon vérifiable, étape par étape, sans aucune approximation.

PHASE 1 **Fondation** **Jours 1—14**	**PHASE 2** **Optimisation** **Jours 15—45**	**PHASE 3** **Résilience des données et de l'activité** **Jours 46—75**	**PHASE 4** **Prouver la valeur** **Jours 76—100**
M1 : Dimensionnement et planification	M4 : Traitement prenant en charge les applications	M7 : Combler les lacunes de couverture	M10 : Test de restauration
M2 : Déploiement de l'appliance Veeam Software et de l'infrastructure Veeam Software	M5 : Copie de sauvegarde, SOBR et Vault	M8 : Résilience face aux ransomwares	M11 : Rapports et documents
M3 : Premières tâches de sauvegarde	M6 : Supervision, alertes et configuration d'Orchestrator	M9 : Optimisation des performances et plans d'orchestration	M12 : Hygiène continue

PHASE 1 • Jours 1 à 14

Fondation

Objectif : infrastructure dimensionnée, déployée et premiers workloads protégés.

Étape 1 : Dimensionnement et planification

Avant de déployer quoi que ce soit, investissez du temps pour dimensionner correctement l'infrastructure. Une infrastructure sous-dimensionnée est la cause la plus fréquente de fenêtres de sauvegarde lentes et du non-respect des RPO au cours des 100 premiers jours.

Inventaire des workloads

- Documentez le nombre total de VM et de workloads, l'empreinte des données (total provisionné vs utilisé) et le taux de modification quotidien estimé.
- Identifiez vos workloads stratégiques, car ce sont eux qui déterminent vos objectifs de RPO et de RTO.
- Notez tous les workloads physiques (p. ex., serveurs Windows/Linux) qui nécessiteront des Veeam Agents.

Dimensionnement de la Veeam Software Appliance

- L'appliance logicielle Veeam est livrée avec Veeam Backup & Replication préinstallé, donc votre principale décision de dimensionnement concerne l'hôte sur lequel elle s'exécute.
- Minimum pour les PME : 8 vCPU/16 Go de RAM (500 Mo de RAM recommandés pour chaque tâche simultanée).
- Utilisez le Calculateur de dimensionnement Veeam (calculator.veeam.com) pour valider les ressources nécessaires pour votre nombre de workloads et votre empreinte de données.
- Choisissez le format de déploiement : une OVA pour VMware vSphere ou une image ISO pour les serveurs physiques et autres hyperviseurs. Aucune expérience Linux n'est requise, quelle que soit la méthode choisie.

Architecture de stockage : choisissez votre voie

À ce stade, votre choix de stockage détermine le reste des phases 1 et 2. Il existe trois options recommandées pour les PME :

Path A : Veeam Software Appliance + Veeam Infrastructure Appliance en tant que Veeam cible renforcée + Vault : il s'agit de la configuration de référence recommandée. Ce chemin d'accès fournit un référentiel local inaltérable sans nécessiter de connaissances approfondies de Linux, ainsi que des copies inaltérables hors site et entièrement isolées logiquement via Vault.

Chemin A : pourquoi utiliser une cible renforcée Veeam fournie via une appliance d'infrastructure Veeam ?

Une cible renforcée Veeam fournit des sauvegardes locales inaltérables. Cela signifie que le ransomware ne peut ni les chiffrer ni les supprimer pendant la période de rétention.

Traditionnellement, un référentiel Linux inaltérable nécessite un serveur Linux dédié et un durcissement manuel du système d'exploitation. La Veeam Infrastructure Appliance élimine entièrement cette contrainte. Elle est livrée pré-renforcée, se déploie à partir d'un fichier OVA ou ISO et ne nécessite aucune connaissance approfondie de Linux pour être déployée ou entretenue.

L'appliance d'infrastructure Veeam est une appliance à rôle unique. Chaque instance s'exécute soit en tant que cible renforcée Veeam, soit en tant que proxy de sauvegarde. Pour les PME sans administrateur Linux dédié ou stockage inaltérable existant, une cible renforcée Veeam fournie par l'appliance Veeam Infrastructure est la solution recommandée pour inaltérabilité locale.

Pour une protection maximale, déployez Veeam Infrastructure Appliance sur du matériel physique. L'exécution de Veeam Infrastructure Appliance en tant qu'appliance virtuelle hérite toujours de la surface d'attaque de l'hyperviseur. L'inaltérabilité au niveau du système de fichiers protège les fichiers de sauvegarde contre les attaques au sein de l'OS, mais un administrateur du hyperviseur peut tout de même supprimer les VM, même si leurs fichiers de sauvegarde sont inaltérables.

Chemin B : Veeam Software Appliance + Veeam Data Cloud Vault : Veeam Backup & Replication écrit les sauvegardes directement sur la cible locale de la Veeam Software Appliance et conserve une copie hors site dans le Veeam Vault. Convient parfaitement aux micro-PME, aux filiales ou aux clients qui souhaitent minimiser la gestion du stockage local, ainsi qu'aux copies inaltérables hors site et entièrement isolées via Vault. Gardez à l'esprit que si une appliance Veeam Software est déployée sur une infrastructure virtuelle, elle ne constitue pas un substitut adéquat à l'inaltérabilité sur site.

Chemin B : pourquoi Veeam Software Appliance + Vault ?

Le chemin B minimise l'administration du stockage. Veeam Backup & Replication écrit les sauvegardes dans une cible locale sur la Veeam Software Appliance elle-même, puis une tâche de copie des sauvegardes les réplique hors site vers Vault.

Le stockage local de l'appliance Veeam Software est inaltérable par défaut, donc le chemin B vous offre toujours une protection sur site contre les ransomwares. Il ne s'agit pas d'une cible renforcée Veeam officielle au sens du produit, donc le chemin A reste le choix le plus solide lorsque vous disposez de matériel à dédier à l'Appliance d'infrastructure Veeam, mais le chemin B est la bonne option lorsque ce n'est pas le cas. Comme pour le chemin A, l'appliance logicielle Veeam Software exécutée en tant qu'appliance virtuelle peut toujours être supprimée au niveau de l'hyperviseur ; déployez-la donc sur du matériel physique chaque fois que c'est possible.

Le chemin B saute entièrement l'étape de la Veeam Infrastructure Appliance. Si vous choisissez cette voie, passez directement de l'étape 2 (déploiement de l'appliance logicielle Veeam Software) à l'étape 5 (tâche de copie de sauvegarde vers le Vault).

Chemin C : Veeam Software Appliance + cible NAS/Windows existante + Vault ou autre stockage hors site tiers : ce chemin utilise l'infrastructure de stockage existante et est moins durci localement, sauf si une configuration supplémentaire est appliquée. Ceci est utile lorsque les clients souhaitent exploiter des partenaires Veeam Cloud & Service Provider (VCSP) existants pour du stockage hors site, ou un stockage hors site alternatif déjà disponible.

Quel que soit votre chemin :

- Envisagez d'isoler le trafic de sauvegarde sur un VLAN ou une carte réseau dédiée afin d'empêcher que les données de sauvegarde ne transitent sur votre réseau de production.
- Vérifiez la couverture de vos licences pour les sockets et les workloads avant le déploiement.

Étape 2 : déploiement de la Veeam Software Appliance et de l'infrastructure

Déployez la Veeam Software Appliance

- Téléchargez l'OVA Veeam Software Appliance (pour VMware vSphere) ou l'ISO (pour les serveurs physiques ou les VM sur d'autres hyperviseurs pris en charge) à partir du portail client Veeam (my.veeam.com).
- Pour OVA : importez dans VMware vSphere et démarrez. Veeam Backup & Replication sera accessible via l'interface de gestion après le premier démarrage.
- Pour ISO : démarrez le serveur cible (par exemple, un serveur physique ou une VM sur un autre hyperviseur pris en charge) à partir de l'image ISO et suivez l'assistant de configuration. Veeam Backup & Replication est installé automatiquement.
- Terminez l'assistant de configuration initiale de Veeam Software Appliance et définissez le nom d'hôte, les paramètres réseau et les informations d'identification administrateur.

Connectez l'infrastructure à Veeam Backup & Replication

- Ajoutez votre plateforme de virtualisation à l'inventaire de Veeam Backup & Replication (infrastructure de sauvegarde > serveurs administrés).
- Ajoutez au moins un proxy de sauvegarde. Dans les petits environnements, Veeam Software Appliance peut servir de proxy initial.
- Pour VMware environnements, configurez le mode de transport avec ajout à chaud. La VM proxy monte les disques source via SCSI et les lit directement, évitant ainsi le chemin NBD plus lent sur le réseau de gestion ESXi.

Déployez l'appliance d'infrastructure Veeam (chemin A)

- Téléchargez le fichier OVA ou ISO de l'appliance Veeam Infrastructure depuis le portail client Veeam.
- Déployez en utilisant le même processus OVA/ISO que pour l'Appliance Veeam Software. Sélectionnez Cible renforcée ou proxy de sauvegarde comme rôle lors de l'exécution de l'assistant de configuration.
- Une fois déployée, ajoutez l'appliance d'infrastructure Veeam à Veeam Backup & Replication en tant que Serveur géré, puis configurez-la comme cible de sauvegarde ou proxy de sauvegarde.

Ce que l'appliance logicielle Veeam Software gère pour vous

Veeam Backup & Replication est préinstallé et prêt à être configuré, sans configuration manuelle de l'OS, ni installation de logiciel, ni correctifs préalables au déploiement.

L'appliance Veeam Software est livrée pré-durcie, les services inutiles sont désactivés, l'OS est verrouillé et les meilleures pratiques de sécurité sont appliquées par défaut.

Déployez en tant qu'OVA sur VMware vSphere, démarrez l'image ISO sur un serveur physique ou démarrez dans une VM sur tout autre hyperviseur pris en charge par Veeam. Aucune expérience Linux n'est nécessaire.

- Pour le rôle de cible renforcée, ajoutez la cible dans Veeam Backup & Replication (« Backup Infrastructure » > « Backup Repositories ») et définissez la période de rétention de l'inaltérabilité.
- Ignorez cette section si vous utilisez le chemin B ou C (car aucune Veeam Infrastructure Appliance n'est requise).

Installez Veeam ONE

- Veeam ONE est un programme d'installation distinct pour Windows. Il n'est actuellement pas fourni dans le cadre du modèle d'appliance.
- Installez Veeam ONE sur une VM Windows Server ou un hôte physique (voir les exigences minimales dans le guide de déploiement de Veeam ONE).
- Connectez Veeam ONE à Veeam Backup & Replication et à votre hôte vCenter/Hyper-V pendant l'assistant d'installation.
- Configurez les paramètres de notification SMTP/e-mail immédiatement après l'installation. Vous voulez que les alertes soient actives dès le premier jour.

Étape 3: Premières tâches de sauvegarde

- Créez votre première tâche de sauvegarde pour votre hyperviseur principal. Ciblez la cible renforcée Veeam (Chemin A), la cible locale sur l'appliance Veeam Software (Chemin B), ou votre cible NAS/Windows existante (Chemin C).
- Définissez une stratégie de rétention judicieuse pour démarrer : 14 points de restauration quotidiens, 4 hebdomadaires, 3 mensuels (GFS).
- Planifiez la tâche pour qu'elle s'exécute pendant les heures creuses et vérifiez qu'elle n'entre pas en conflit avec d'autres fenêtres de maintenance.
- Exécutez la tâche manuellement lors de la première exécution et surveillez-la jusqu'à son terme.
- Vérifiez que la tâche s'est achevée sans avertissement ni erreur avant de passer à la phase 2.

Premier test de restauration — ne sautez pas cette étape !

Avant de passer à la phase 2, effectuez un Instant VM Recovery pour une VM non critique afin de confirmer la capacité de restauration.

Vous n'êtes pas protégé tant que vous n'avez pas vérifié votre capacité à restaurer. Cela ne prend que quelques minutes et peut vous éviter des jours de problèmes par la suite.

Ce que la Veeam Infrastructure Appliance prend en charge pour vous

À l'instar de la Veeam Software Appliance, la Veeam Infrastructure Appliance est livrée pré-durcie et préconfigurée pour le rôle qui lui est attribué. Aucune administration Linux n'est nécessaire après le déploiement.

Une seule appliance d'infrastructure Veeam remplit un seul rôle : cible renforcée Veeam ou proxy de sauvegarde. Si vous avez besoin des deux, déployez deux appliances.

Les formats de déploiement sont les mêmes que ceux de Veeam Software Appliance : OVA pour VMware vSphere, ou ISO pour les serveurs physiques et autres hyperviseurs pris en charge.

PHASE 2 • Jours 15 à 45

Optimisation

Objectif : protection constante, copie hors site et visibilité dans l'ensemble de l'environnement.

Étape 4 : Traitement prenant en charge les applications

Le traitement prenant en charge les applications garantit que les sauvegardes cohérentes en cas d'incident deviennent également cohérentes au niveau des applications. C'est essentiel pour les workloads transactionnels tels que SQL Server, Oracle, Exchange, Active Directory et d'autres workloads applicables.

- Activez le traitement invité dans les tâches de sauvegarde couvrant des serveurs d'applications Windows ou Linux.
- Configurez le traitement prenant en charge les applications pour SQL Server, Oracle, Exchange, les contrôleurs de domaine Active Directory et les autres workloads applicables.
- Définissez une politique de troncature des journaux de transactions, le cas échéant et en fonction de vos besoins de restauration.
- Après la première exécution de la tâche prenant en charge les applications, confirmez que les points de restauration sont marqués comme cohérents au niveau des applications dans Veeam Sauvegarde & Réplication.
- Testez une restauration au niveau objet d'une base de données SQL (ou d'autres workloads applicables) à l'aide de Veeam Explorer for Microsoft SQL Server pour confirmer que la restauration de l'application de bout en bout fonctionne.

Étape 5 :
Copie de sauvegarde et Vault

Ce jalon complète votre stratégie 3-2-1 : une copie locale sur votre cible principale, plus une copie inaltérable hors site. C'est la pierre angulaire de l'architecture de votre environnement de sauvegarde.

Connectez Vault

- Ajoutez Vault en tant que cible de stockage objet dans Veeam Backup & Replication (Infrastructure de sauvegarde > Cibles de stockage objet).
- Connectez-vous à l'aide de vos informations d'identification délivrées par Veeam et sélectionnez votre région.
- Vérifiez que l'inaltérabilité est activée.

Tâches de copie de sauvegarde

- Configurez les tâches de copie des sauvegardes avec une stratégie de rétention GFS pour maintenir des points de restauration à long terme hors site.
- Vérifiez que les tâches de copie des sauvegardes hors site aboutissent avec succès et que les objets Vault affichent des indicateurs d'inaltérabilité dans Veeam Backup & Replication.
- Effectuez un test de restauration à partir de Vault pour confirmer que la copie hors site est accessible avant de déclarer la phase 2 terminée.

Chemin C : options de destination hors site

Les chemins A et B ciblent tous deux Vault pour la copie hors site. Le chemin C peut utiliser Vault ou un VCSP alternatif, ou une cible hors site tiers si vous en avez déjà une en place. L'inaltérabilité est appliquée par défaut à toutes les données de sauvegarde stockées dans Vault. Si vous ciblez un référentiel hors site non-Vault, vérifiez que l'inaltérabilité ou le verrouillage d'objet est configuré sur ce référentiel.

Étape 6 : Supervision, alertes et configuration de l'Orchestrator

- Configurez les destinataires des notifications d'alerte dans Veeam ONE : alertes par e-mail en cas d'échecs de tâches et de non-respect des contrat de niveau de service (S.L.A.).
- Définissez les horaires de fonctionnement dans Veeam ONE afin d'aligner le calcul des SLA sur votre calendrier opérationnel.
- Passez en revue les seuils d'alerte par défaut : désactivez ou modifiez les alertes non pertinentes pour votre environnement afin d'éviter la fatigue liée aux alertes.
- Générez vos premiers rapports Veeam ONE : rapport sur les VM protégées et rapport sur les sessions de tâche.
- Examinez le rapport des VMs non protégées et corrigez toutes les lacunes identifiées avant de passer à la phase 3.

Installez Veeam Recovery Orchestrator (réservé à la version Premium)

Ignorez cette section si votre édition est Foundation ou Advanced. Veeam Recovery Orchestrator est uniquement inclus avec Veeam Data Platform Premium.

- Veeam Recovery Orchestrator est un programme d'installation Windows distinct. Il peut se trouver avec Veeam ONE sur le même hôte Windows ou être exécuté sur son propre hôte.
- Installez Veeam Recovery Orchestrator sur une VM Windows Server ou un hôte physique. Référez-vous aux exigences minimales dans le guide de déploiement de Veeam Recovery Orchestrator.
- Pendant l'assistant d'installation, connectez Veeam Recovery Orchestrator à votre instance Veeam Backup & Replication afin qu'il puisse inventorier vos chaînes de sauvegarde existantes.
- Connectez Veeam Recovery Orchestrator à votre vSphere, Hyper-V ou Microsoft Azure afin que votre exécution planifiée puisse mettre sous tension les VM et attribuer les réseaux correctement.
- Optionnellement, connectez Veeam Recovery Orchestrator à Veeam ONE pour des données de supervision plus riches et une vérification basée sur DataLab.
- Activez votre licence Veeam Data Platform Premium pour activer Veeam Recovery Orchestrator.
- Configurez SMTP/e-mail afin que les notifications d'exécution planifiée fonctionnent dès le premier jour.

PHASE 3 • Jours 46—75

Résilience des données et résilience de l'activité

Objectif : combler les lacunes en matière de protection, améliorer les RTO/RPO et renforcer la résilience face aux ransomwares.

Étape 7 : Combler les lacunes en matière de couverture

- Exécutez le rapport des VMs non protégées dans Veeam ONE pour traiter tous les workloads non protégés avant tout autre paramétrage.
- Étendez la protection aux workloads physiques en utilisant Veeam Agent *pour Microsoft Windows* ou Veeam Agent *pour Linux*, selon vos besoins.
- Examinez les plannings des tâches pour détecter les conflits et échelonnez les heures de démarrage afin d'éviter la contention des ressources entre les proxys et les cibles.
- Validez la conformité RPO : toutes les VMs critiques génèrent-elles des points de restauration dans votre fenêtre de restauration cible ?
- Vérifiez que toutes les tâches s'effectuent dans les limites de la fenêtre de sauvegarde définie.

Ajout de capacité de proxy avec un second VIA

Si les tâches de sauvegarde s'exécutent lentement ou dépassent leur fenêtre de sauvegarde, déployez une seconde appliance d'infrastructure Veeam dans le rôle proxy.

Grâce au modèle d'appliance pré-renforcée, la mise en œuvre est rapide : déployez l'OVA ou l'ISO, enregistrez-le dans Veeam Backup & Replication, et l'équilibrage de charges se fera automatiquement entre les deux proxys, sans configuration manuelle requise.

Étape 8 : Préparation au ransomware

- Les éditions Advanced et Premium de la Veeam Data Platform sont livrées avec deux outils de sécurité complémentaires. Le premier est Recon, le service de renseignements sur les menaces de Veeam, qui met en évidence les IOC et les données émergentes issues de réponses aux incidents réelles. Le deuxième est l'analyse de sauvegarde, une action intégrée au produit dans Veeam Backup & Replication. Elle examine les chaînes de sauvegarde existantes à la recherche d'indicateurs de logiciels malveillants et valide l'intégrité des fichiers, sans nécessiter de réseau isolé ni le démarrage des VM.

Exécutez une analyse de sauvegarde :

- Créez une tâche SureBackup dans Veeam Backup & Replication sous « Accueil » > « SureBackup ». SureBackup® s'exécute en tant que tâche planifiée et peut analyser vos sauvegardes à la recherche de logiciels malveillants, de menaces à base de signatures et de l'intégrité des fichiers, le tout en un seul processus, sans nécessiter de réseau isolé ni le démarrage d'une VM pour l'analyse elle-même.

- Associez les tâches de sauvegarde que vous souhaitez couvrir afin que, au fil du temps, la tâche SureBackup® englobe toutes vos données : cible renforcée Veeam (chemin A), cible locale de l'appliance Veeam Software (chemin B), cible NAS/Windows existante (chemin C) et Vault.
- Dans les options de vérification, activez la recherche de logiciels malveillants avec Veeam Threat Hunter (ou une solution antivirus tierce) pour examiner le contenu des sauvegardes par rapport à une base de données de signatures de menaces à jour.
- Dans les mêmes options de vérification, activez la vérification d'intégrité des fichiers pour valider le fichier de sauvegarde avec une vérification CRC afin d'identifier les blocs corrompus.
- Planifiez le job SureBackup® et examinez régulièrement les résultats de session ; investiguez tout point de restauration signalé avant de l'utiliser pour la restauration.
- Pour effectuer une vérification ad hoc entre des exécutions programmées, rendez-vous dans Accueil > Sauvegardes, développez la tâche de sauvegarde, sélectionnez le workload, puis choisissez Analyser la sauvegarde dans l'onglet Sauvegarde.

Installez Recon

- Installez le binaire Recon sur n'importe quel hôte d'infrastructure Windows Veeam ou sur tout hôte Linux de votre choix.
- Recon peut également être installé sur les contrôleurs de domaine Windows applicables.
- Recon ne peut pas être installé sur l'appliance d'infrastructure Veeam. Les Veeam Infrastructure Appliances sont à rôle unique et pré-renforcées.

Audit de l'inaltérabilité

- Confirmez que la période d'inaltérabilité sur la cible renforcée de votre Veeam Infrastructure Appliance est définie sur une fenêtre de rétention appropriée.
- Examinez les paramètres de chiffrement des sauvegardes et activez le chiffrement au repos pour les tâches si ce n'est pas déjà fait.
- Lancez le rapport Veeam ONE « workloads inaltérables » pour mesurer et identifier les objectifs d'inaltérabilité des sauvegardes de workloads.

Préparation à la restauration après une attaque par ransomware

Documentez un runbook de restauration simple qui précise quelles VM restaurer en premier, à partir de quels points de restauration, et vers quelle cible.

Identifiez au moins un point de restauration sain, antérieur à l'infection, dans Vault comme votre dernier point d'ancrage sain connu.

Vos sauvegardes immuables ne peuvent pas être écrasées ou chiffrées pendant la période d'inaltérabilité. C'est votre filet de sécurité.

Chemin A : cible renforcée Veeam plus Vault.

Chemin B : stockage local de l'appliance Veeam Software plus Veeam Vault.

Chemin C : Vault plus votre cible locale si vous y avez configuré l'inaltérabilité.

Étape 9: Optimisation des performances et plans d'orchestration

- Examinez le débit du proxy dans les statistiques des tâches Veeam Backup & Replication. Si les tâches sont en goulot d'étranglement, déployez une deuxième appliance d'infrastructure Veeam dans le rôle de proxy.
- Vérifiez que le mode de transport des sauvegardes est optimal : ajout à chaud (VMware) ou accès direct au stockage si disponible.
- Validez que toutes les tâches de sauvegarde sont achevées dans la fenêtre de maintenance que vous avez définie.
- Examinez les graphiques de performance de Veeam ONE et identifiez les VM présentant des taux de changement anormalement élevés, qui pourraient bénéficier de tâches dédiées ou de plannings ajustés.

Créez des plans d'orchestration initiaux (Premium uniquement)

Ignorez cette section si votre édition est Foundation ou Advanced, ou si vous n'utilisez pas d'hyperviseur pris en charge pour Veeam Recovery Orchestrator.

Veeam Recovery Orchestrator transforme votre runbook de restauration manuelle en plan exécutable. La création de plans dès maintenant permet à la phase 4 de vérifier automatiquement la capacité de restauration, plutôt que de relancer des restaurations manuelles.

- Identifiez les ensembles applicatifs de niveau 1 nécessitant une restauration orchestrée (p. ex., contrôleurs de domaine, base de données principale, serveurs applicatifs principaux).
- Dans Veeam Recovery Orchestrator, créez votre premier plan de restauration couvrant l'une de ces piles applicatives.
- Définissez l'ordre de démarrage et les dépendances de vos VM afin que les prérequis (p. ex., les contrôleurs de domaine, DNS, etc.) démarrent avant les services dépendants.
- Configurez les cibles de restauration (p. ex., hôte, cluster, datastore) et cartographiez le réseau de production pour un basculement effectif, ainsi qu'un réseau isolé pour les tests.
- Définissez les objectifs RTO et RPO du plan afin que Veeam Recovery Orchestrator puisse signaler les dérives au fil du temps.
- Enregistrez le plan et examinez la documentation générée automatiquement avec les parties prenantes avant de déclarer la phase 3 terminée.

PHASE 4 • Jours 76 à 100

Démontrez la valeur et opérationnalisez

Objectif : vérifier la capacité de restauration, établir une hygiène continue et démontrer le ROI.

Étape 10 : Tests de restauration

La seule sauvegarde qui compte est celle dont vous pouvez restaurer les données. La phase 4 est celle où vous démontrez, preuves documentées à l'appui, que votre environnement respecte ses engagements en matière de RTO et de RPO.

SureBackup et analyse de sauvegarde

- Configurez un groupe d'applications SureBackup qui couvre vos VM les plus critiques (p. ex., contrôleurs de domaine, serveurs d'applications clés).
- Exécutez un job SureBackup® pour automatiser la vérification du démarrage et confirmer que les VM démarrent et réussissent les tests de heartbeat, de ping et au niveau application.
- Pour une passe de vérification plus légère, exécutez une analyse de sauvegarde. Il valide l'intégrité des fichiers et vérifie les menaces sans démarrer les VM, ce qui constitue un complément pratique à SureBackup® ou une autre solution dans les petits environnements.

Tests de restauration granulaire et complète

- Testez des restaurations au niveau fichier et restaurez des fichiers individuels depuis une sauvegarde vers un emplacement de test.
- Testez la restauration d'un objet applicatif en restaurant un objet de base de données SQL ou un compte utilisateur Active Directory à l'aide de Veeam Explorers™.
- Testez une restauration de VM entière à partir de Vault pour simuler une perte totale sur site et valider la copie hors site.
- Enregistrez les temps de restauration réels, comparez-les à vos objectifs de RTO et documentez les résultats.

Meilleures pratiques pour les tests de restauration

Restaurez toujours vers une cible hors de production et n'écrasez jamais les workloads actifs pendant un test.

Documentez ce qui a été restauré, à partir de quel point de restauration, sur quelle cible et combien de temps cela a pris.

Ces résultats constituent la preuve de votre capacité de restauration. Conservez-les pour vos besoins d'examens de conformité, d'audits et de reporting de gestion.

Exécuter des plans d'orchestration (Premium uniquement)

Ignorez cette section si votre édition est Foundation ou Advanced, ou si votre hyperviseur n'est pas pris en charge par Veeam Recovery Orchestrator. La phase 3 a établi votre premier plan de restauration, mais c'est en phase 4 qu'il démontre toute son utilité.

- Exécutez un test de préparation sans surveillance sur votre plan. Veeam Recovery Orchestrator vérifie la disponibilité des points de restauration, la capacité cible et la dérive de configuration, sans nécessiter le démarrage des VM.
- Exécutez un test DataLab sur votre plan. Veeam Recovery Orchestrator restaure la pile applicative dans un réseau isolé et effectue des vérifications de niveau applicatif sur des VM dynamiques.
- Enregistrez les temps de restauration réels à partir de l'exécution de DataLab et comparez-les à l'objectif RTO que vous avez défini lors de la phase 3.
- Générez le rapport de préparation à la restauration de Veeam Recovery Orchestrator et archivez-le avec les autres rapports de tests de restauration.
- Pour les workloads non couverts par un plan Veeam Recovery Orchestrator, revenez aux tests de restauration manuelle ci-dessus.

Étape 11 : Rapports et documentation

Générez un rapport mensuel de synthèse Veeam ONE et communiquez-le à la direction pour démontrer l'intégrité et la couverture de la sauvegarde.

- Exportez un rapport d'inventaire des workloads protégés afin de vérifier l'étendue de la couverture.
- Documentez votre architecture de sauvegarde finale, y compris la liste des tâches, la structure des cibles, les rôles des appliances d'infrastructure Veeam, les planifications et les stratégies de rétention.
- Examinez la consommation de stockage Veeam Vault et confirmez que votre utilisation correspond à votre budget prévisionnel.
- Archivez les résultats des tests de restauration avec la documentation de l'architecture.
- Premium uniquement : générez chaque mois le rapport sur l'état de préparation à la restauration de Veeam Recovery Orchestrator. Suivez le score de préparation au fil du temps, à mesure que les workloads et les dépendances évoluent.
- Premium uniquement : archivez la documentation du plan générée par Veeam Recovery Orchestrator avec les documents de votre architecture. Veeam Recovery Orchestrator régénère automatiquement cette documentation lorsque les plans changent ; pensez donc à la réarchiver lorsque les plans sont mis à jour.

Étape 12 : cadence d'hygiène continue

Au 100e jour, votre environnement devrait être stable et entièrement documenté. Ces habitudes permettent de maintenir cet état :

- **Chaque semaine :** consultez le tableau de bord d'intégrité de vos tâches Veeam ONE et traitez rapidement les échecs ou les avertissements.
- **Chaque semaine :** examinez le rapport des VM non protégées dans Veeam ONE et ajoutez une protection pour tout ce qui est nouveau.
- **Chaque mois :** produisez un rapport résumé et des rapports des VM protégées, puis partagez les résultats.
- **Chaque mois :** examinez la consommation et le taux de croissance du stockage Vault. Signalez-le si vous dépassez l'empreinte budgétisée ou si une augmentation de la rétention est imminente.
- **Chaque mois :** confirmez que les fenêtres de rétention sont toujours actives et non modifiées.
- **Chaque trimestre :** effectuez un test de restauration documenté et alternez les types de workload.
- **Chaque trimestre :** effectuez une analyse de sauvegarde sur chaque cible afin de vérifier la présence de signatures de logiciels malveillants et de variations de l'intégrité des fichiers.
- **Trimestriellement :** vérifiez qui dispose d'un accès administratif à Veeam Backup & Replication, Veeam ONE et Veeam Recovery Orchestrator (Premium uniquement). Retirez l'accès à toute personne ayant changé de rôle ou ayant quitté l'organisation.
- **Chaque trimestre (Premium uniquement) :** effectuez un test DataLab de Veeam Recovery Orchestrator et alternez le plan d'orchestration exercé.
- **Chaque trimestre (Premium uniquement) :** régénérez et archivez la documentation des plans Veeam Recovery Orchestrator si des plans ont changé depuis le dernier examen.
- **Chaque mois :** passez en revue les mises à jour de Recon Threat Intelligence et appliquez les signatures ou les règles pertinentes à votre environnement.

- **Annuellement :** examinez votre architecture de sauvegarde et vos stratégies de rétention par rapport aux exigences métier actuelles et à toute nouvelle obligation de conformité.

- **Annuellement :** effectuez une restauration complète depuis Vault pour vérifier que la copie hors site est restaurable de bout en bout. Documentez le résultat.

- **Annuellement :** vérifiez les paramètres de chiffrement en cours de transfert et sur la cible et effectuez la rotation des clés conformément à votre politique de sécurité.

- **Selon vos besoins :** planifiez la fréquence de mise à jour de vos composants Veeam (par exemple, Veeam Software Appliance, Veeam Infrastructure Appliance, Veeam ONE, Veeam Agents et Veeam Recovery Orchestrator, le cas échéant) et abonnez-vous aux notifications de publication.

- **Avant le renouvellement :** examinez l'utilisation des licences, les prévisions de croissance et la pertinence de l'édition. Si vous avez dépassé les fonctionnalités de votre édition, c'est le moment de discuter d'une mise à niveau avec votre représentant Veeam.

Recommandations finales

Félicitations ! Vous l'avez fait.

En 100 jours, vous êtes passé du déploiement à un environnement de protection des données pleinement opérationnel. Vos workloads sont protégés, vos sauvegardes sont durcies et inaltérables, et vous avez prouvé, preuve à l'appui, que vous pouvez restaurer, non seulement en théorie, mais de façon vérifiable.

Ce n'est pas rien.

À présent, l'accent passe de la construction à la maintenance. Maintenez les restaurations sur un calendrier de tests régulier, ajustez les politiques à mesure que votre environnement évolue, et utilisez votre cadence de supervision et de reporting pour détecter toute dérive avant qu'elle ne devienne un risque. Les habitudes que vous avez établies lors de l'étape 12 — votre routine de vérification hebdomadaire, mensuelle, trimestrielle et annuelle — sont ce qui garantit l'intégrité de votre environnement bien après le centième jour. Suivez-les, adoptez-les et faites-les évoluer à mesure que votre organisation grandit.

N'oubliez pas que le jour 100 n'est pas la ligne d'arrivée. C'est la référence de base. La résilience est une pratique, pas un projet.

Gardez vos rôles d'administrateur à jour pour que les bonnes personnes aient toujours le bon accès, et restez abonné aux notes de publication et aux avis de sécurité Veeam afin de ne jamais être pris au dépourvu.

Vous n'avez pas à faire cela seul

Les communautés, les ressources pédagogiques et les équipes techniques de Veeam existent pour vous aider à aller plus loin. Exploitez-les à mesure que votre environnement se développe et gagne en maturité ! Une liste de ressources soigneusement sélectionnées est disponible en annexe.

Pour toute question ou pour connaître les prochaines étapes, contactez votre Responsable de la réussite client ou le support technique de Veeam pour toute demande technique.

Annexe : Référence rapide

Composants clés : Veeam Data Platform

- **Appliance logicielle Veeam :** une appliance pré-renforcée avec Veeam Backup & Replication préinstallé. Déploiement sous forme d'OVA (VM) ou d'ISO (physique). C'est le point de départ recommandé pour tous les déploiements par des PME.
- **Veeam infrastructure Appliance :** une appliance pré-durcie déployée en tant que proxy de sauvegarde dédié ou cible renforcée. Elle assure l'inaltérabilité locale, sans connaissance approfondie de Linux, chaque appliance étant liée à un seul rôle.
- **Veeam Backup & Replication :** un moteur de sauvegarde central, hébergé sur une Veeam Software Appliance. Il gère les tâches, les cibles, les proxys et les opérations de restauration.
- **Veeam ONE :** assure la supervision, l'alerte et le reporting. Veeam ONE dispose d'une installation distincte sous Windows et se connecte à Veeam Backup & Replication ainsi qu'à votre hyperviseur pour une visibilité complète de la pile.
- **Recon :** il s'agit du service de renseignements sur les menaces de Veeam. Il met en évidence des indicateurs de compromission (IOC), des signatures de menaces et des données de campagnes émergentes issues d'incidents réels. Inclus avec Veeam Data Platform Advanced.
- **Analyse du contenu des sauvegardes :** il s'agit d'une action intégrée au produit qui analyse les chaînes de sauvegarde existantes à la recherche de signatures de logiciels malveillants connues et valide l'intégrité des fichiers, sans nécessiter d'isoler le réseau ni de démarrer les VM. Inclus avec Veeam Data Platform Advanced.
- **Veeam Recovery Orchestrator :** une plateforme d'orchestration qui automatise la reprise après incident au niveau application (DR). Il vous permet de créer des plans de restauration exécutables, d'effectuer des tests de préparation, de réaliser des vérifications basées sur DataLab et de générer la documentation de restauration. Inclus avec Veeam Data Platform Premium.
- **Veeam Data Cloud Vault :** offre un stockage objet inaltérable dans le cloud pour les copies hors site. Elle est gérée par Veeam, aucun compte cloud distinct n'est requis.

Termes clés

- **Délai optimal de reprise d'activité (RPO) :** pertes de données maximales acceptables, mesurées en temps. Détermine la fréquence des sauvegardes.
- **Objectif de temps de restauration (RTO) :** temps d'arrêt maximal acceptable avant qu'un workload ne doive être restauré.
- **Grandfather-Father-Son (GFS) :** schéma de rétention conservant des points de restauration quotidiens, hebdomadaires et mensuels.
- **Inaltérabilité :** données de sauvegarde impossibles à modifier ou à supprimer pendant une période de rétention définie. Protège contre le chiffrement des fichiers de sauvegarde par les ransomwares.
- **Instant VM Recovery :** restaure une VM directement à partir d'une sauvegarde en quelques secondes sans avoir à copier les données au préalable. Toujours faire migrer vers le stockage de production après validation.
- **Plan d'orchestration (Veeam Recovery Orchestrator) :** un runbook exécutable qui définit l'ordre, les dépendances, les emplacements cibles et les mappages réseau pour restaurer un ensemble de workloads. Remplace un runbook de restauration manuel par une automatisation documentée automatiquement et testable.
- **DataLabs :** un environnement de test isolé permettant à Veeam Recovery Orchestrator (ou SureBackup®) de restaurer une sauvegarde et d'effectuer une vérification au niveau de l'application sans impacter la production. Permet de tester l'ensemble du plan à la fréquence de votre choix.
- **Traitement prenant en charge les applications :** traitement de la machine invitée qui crée des points de sauvegarde cohérente de l'application pour SQL Server, Oracle, Exchange, Active Directory, SharePoint, PostgreSQL et MySQL. Utilise VSS sur Windows et des scripts de pre-freeze et post-thaw ainsi que la quiescence native des bases de données sur Linux.
- **Cible renforcée Veeam :** une cible de sauvegarde basée sur Linux avec l'inaltérabilité appliquée au niveau du système de fichiers. Veeam Infrastructure Appliance fournit une cible renforcée Veeam préconfigurée, sans administration de Linux requise. Le stockage objet et le verrouillage des objets sont des mécanismes d'inaltérabilité distincts, et non des cibles renforcées Veeam. L'inaltérabilité au niveau du système de fichiers protège contre les attaques dans le système d'exploitation, mais pas contre la destruction des VM. Une cible renforcée Veeam exécutée sous forme d'appliance virtuelle peut toujours être supprimée au niveau de l'hyperviseur ; déployez donc l'appliance d'infrastructure Veeam sur du matériel physique pour une protection maximale.
- **Mode de transport par ajout à chaud :** il s'agit d'un mode de transport de sauvegarde spécifique à VMware. La VM proxy ajoute à chaud les disques virtuels de la VM source et les lit via SCSI, évitant ainsi le chemin NBD sur le réseau de gestion ESXi.

Annexe : Liens utiles

Mon compte

Votre compte Veeam est votre point central pour gérer votre déploiement. Une fois connecté, vous pouvez télécharger les produits et les clés de licence, gérer les administrateurs du support, contacter le support Veeam, et renouveler des contrats ou ajouter des licences.

- Connectez-vous ou créez votre compte Veeam
- Comment créer un compte
- FAQ dédiée à la connexion
- Administration de licence et/ou de dossier

Documentation et téléchargements

- Centre d'assistance avec documentation technique, instructions de déploiement et guides de l'utilisateur
- Téléchargements de produits, y compris mises à jour logicielles, correctifs et notes de publication
- Base de connaissances du support avec les problèmes courants, les étapes de dépannage et les solutions recommandées, régulièrement mises à jour par les équipes de support et d'ingénierie de Veeam

Apprentissage et meilleures pratiques

- Webinaires d'intégration réguliers en direct : des webinaires où vous pouvez poser vos questions en temps réel et échanger directement avec des spécialistes techniques
- Veeam University FREE : cours en autonomie et certifications gratuites
- Calculateurs de dimensionnement Veeam : outil en ligne de dimensionnement et d'estimation utilisé pour calculer les besoins d'infrastructure, de stockage et de capacité pour les déploiements Veeam
- Bonnes pratiques par les architectes de solutions Veeam : conseils de conception et de configuration de l'infrastructure issus de déploiements réels, qu'il vaut la peine de revoir à mesure que votre environnement évolue.
- Prompts pratiques pour Veeam Intelligence : une collection organisée de prompts efficaces pour vous aider à exploiter tout le potentiel de Veeam Intelligence
- Veeam Search : portail de recherche centralisé de Veeam pour effectuer des recherches dans l'ensemble des ressources Veeam à partir d'un emplacement unique

Communautés Veeam

- Forums de la communauté Veeam : communiquez avec vos homologues, partagez vos meilleures pratiques, inscrivez-vous à des groupes d'utilisateurs, participez à des événements de la communauté et discutez de cas d'utilisation réels.
- Forums R&D de Veeam : votre ligne directe avec l'équipe R&D de Veeam pour des discussions sur les produits, des questions techniques et des retours sur les fonctionnalités

À propos de Veeam Software

Veeam, acteur de référence de la confiance des données et de l'IA, est une société spécialisée dans l'aide aux organisations pour garantir que leurs données et leur IA sont pleinement comprises, sécurisées et résilientes, afin de pouvoir accélérer leur innovation en matière d'IA sécurisée à grande échelle. En tant que leader du marché en matière de résilience des données et de gestion de la posture de sécurité des données, Veeam est conçu pour la convergence de l'identité, des données, de la sécurité et des risques liés à l'IA.

Basé à Seattle et possédant des bureaux dans plus de 30 pays, Veeam protège plus de 550 000 clients dans le monde, dont 82 % des entreprises du Fortune 500.

Pour en savoir plus, rendez-vous sur www.veeam.com ou suivez Veeam sur LinkedIn @veeam-software et X @veeam.