OBJECT FIRST

White Paper

Zero Trust et la sauvegarde des données d'entreprise

Application des principes Zero Trust à la résilience des données

Zero Trust et la sauvegarde/ restauration des données

Le modèle Zero Trust s'impose comme la meilleure pratique actuelle pour les organisations qui cherchent à protéger et à sécuriser leurs informations et leurs activités. Cependant, ce modèle reste peu appliqué à la sauvegarde et à la restauration des données. Ensemble, le cabinet de conseil en Zero Trust Numberline Security et Veeam ont récemment mené des recherches afin de combler cette lacune et de réduire les risques pour les organisations cherchant à évoluer au-delà de la sécurité périmétrique. Ces travaux ont fait naître un nouveau modèle : la résilience des données Zero Trust (Zero Trust Data Resilience, ou ZTDR).

La ZTDR s'appuie sur le **Zero Trust Maturity Model (ZTMM)** de la Cybersecurity and Infrastructure Security Agency (CISA), en étendant ses principes à la sauvegarde et à la restauration des données d'entreprise.

Le cadre ZTDR est un guide pratique destiné aux équipes IT et sécurité visant à améliorer la protection des données, à réduire les risques de sécurité et à renforcer la cyberrésilience des organisations.

Les cyberattaques et les ransomware ciblent les données de sauvegarde dans 93 % des attaques.

Les données de sauvegarde sont souvent la cible principale des ransomware et des attaques d'exfiltration de données ; malheureusement, les cadres Zero Trust existants n'incluent pas la sécurité des systèmes de sauvegarde et de restauration des données.

Le document de recherche original, « Zero Trust Data Resilience — A Secure Data Backup and Recovery Model », est disponible ici :

https://go.veeam.com/zero-trust-data-resilience

Principes Zero Trust

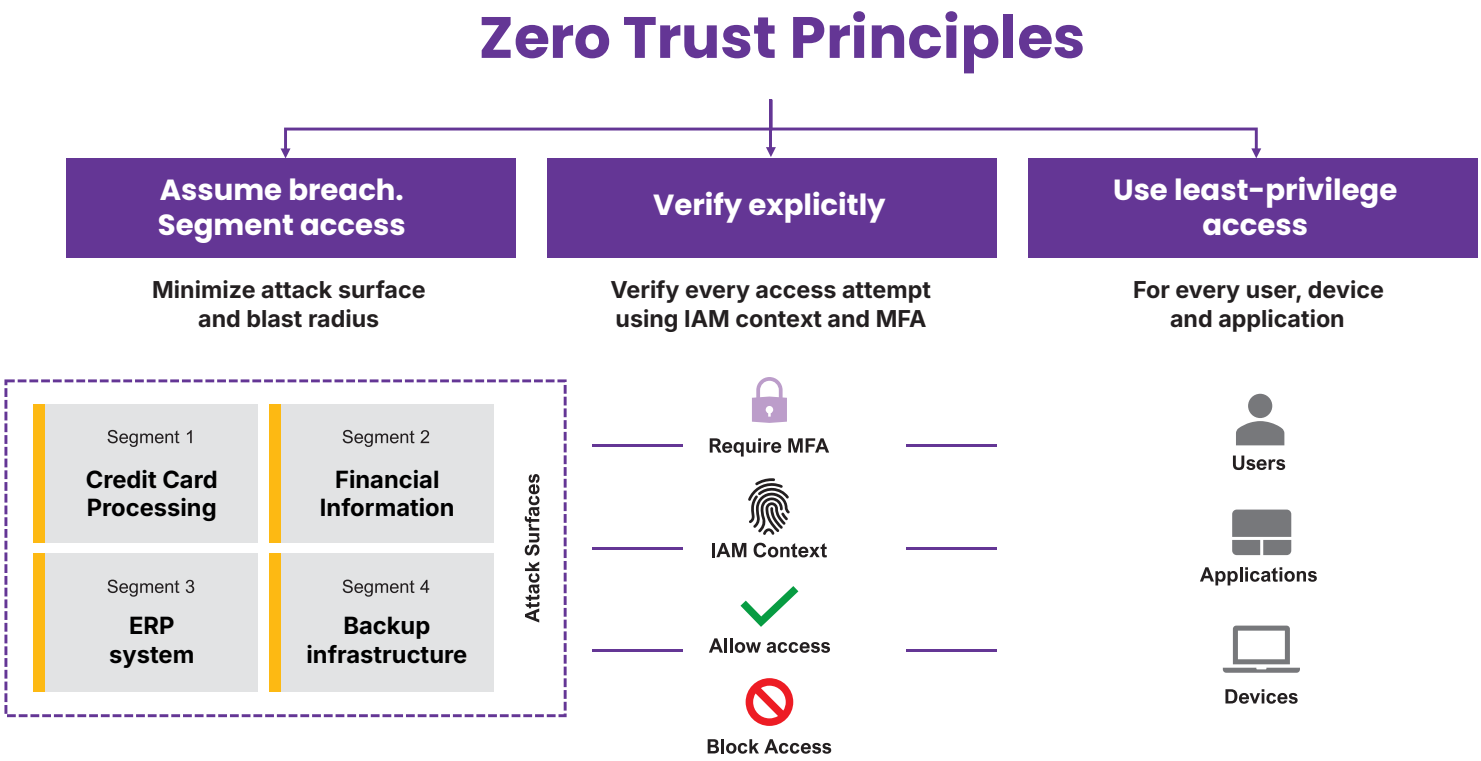
Le Zero Trust est un modèle de sécurité qui remplace l'approche classique de sécurité périmétrique, devenue de plus en plus inefficace. Pour le gouvernement américain et les entreprises du monde entier qui commencent à l'appliquer, le Zero Trust s'impose comme la norme de sécurité informatique de référence.

Le concept s'applique universellement aux organisations qui opèrent sur site, dans le cloud et dans des environnements hybrides, indépendamment de leur taille ou de leur secteur d'activité.

Les grands principes du Zero Trust sont les suivants :

- **Présumer l'existence d'une intrusion. Segmenter l'accès** aux données les plus critiques afin de minimiser la surface d'attaque et le champ d'action de chaque segment.
- **Vérifier explicitement.** L'authentification et les autorisations doivent toujours s'appuyer sur la gestion des identités et des accès (IAM), le contexte (lieu, heure, etc.) et l'authentification forte par MFA.
- **Adopter le principe du moindre privilège** pour chaque utilisateur, appareil et application.

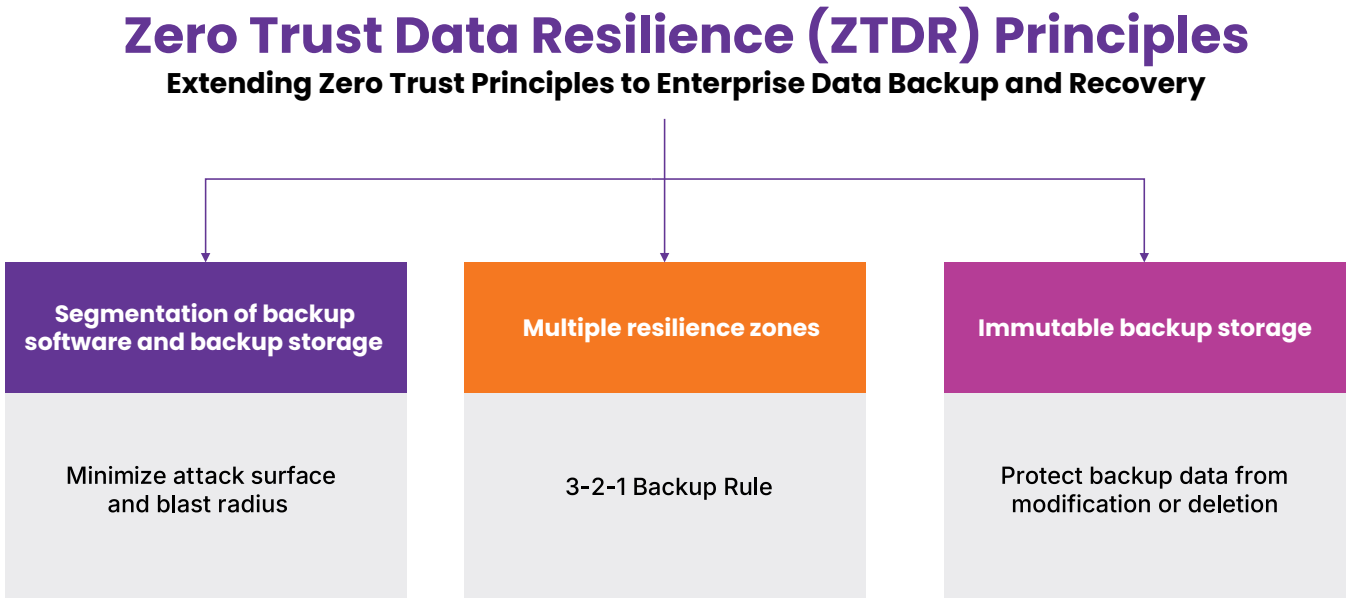
En outre, le Zero Trust exige une visibilité et une analyse continues de la sécurité, l'automatisation et l'orchestration, ainsi que la gouvernance pour la gestion du cycle de vie des données.



Principes ZTDR

Les recherches menées sur la résilience des données Zero Trust introduisent les principes ZTDR suivants qui étendent le Zero Trust à la sauvegarde/restauration des données d'entreprise :

- **Segmentation — Séparation du logiciel et du stockage de sauvegarde** afin d'appliquer le principe de moindre privilège et de minimiser la surface d'attaque et l'étendue des dégâts.
- **Plusieurs zones de résilience des données ou domaines de sécurité** pour respecter **lla règle de sauvegarde 3-2-1** et assurer une sécurité multicouche.
- **Stockage de sauvegarde immuable** pour protéger les données de sauvegarde contre les modifications et les suppressions. Pour **une véritable immuabilité,** il est indispensable de garantir **zéro accès au compte ROOT et au système d'exploitation,** afin de protéger le système contre les attaquants externes et les administrateurs compromis.



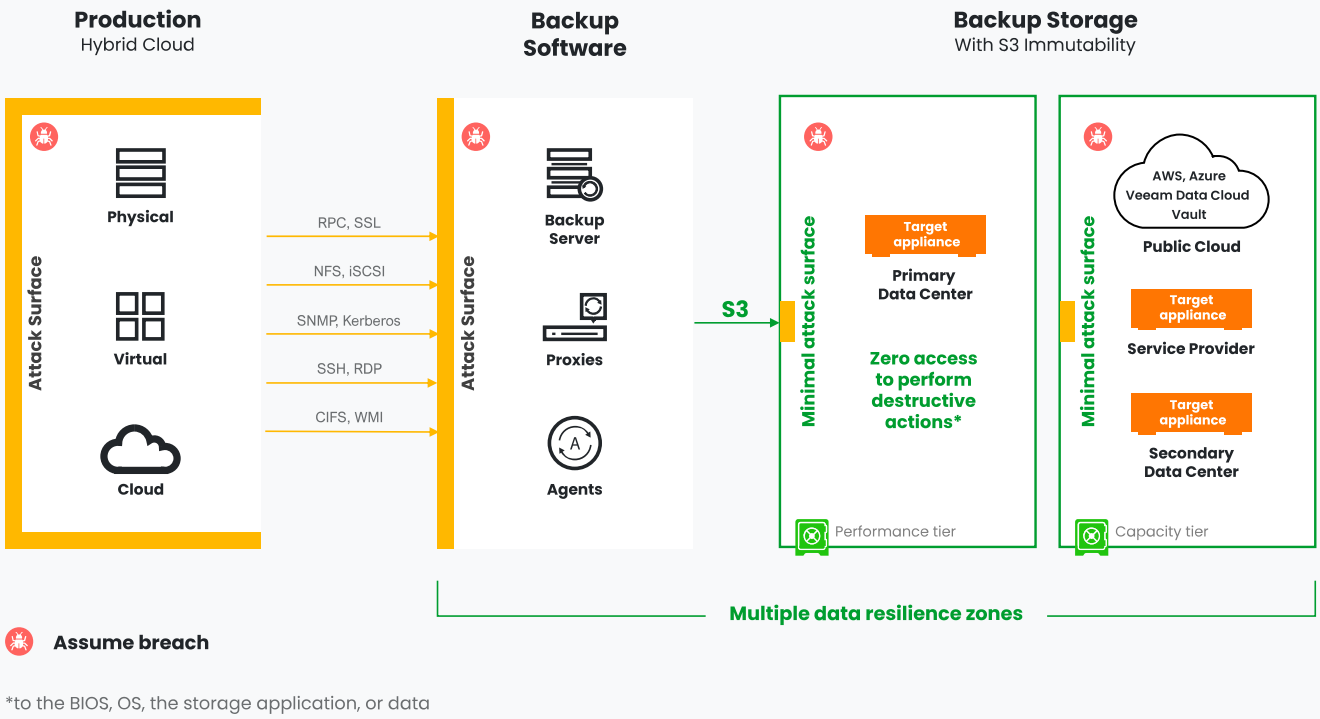
Séparation du logiciel et du stockage de sauvegarde

Par nature, l'infrastructure de sauvegarde présente une grande surface d'attaque, car elle nécessite un accès en lecture et en écriture aux systèmes de production sur l'ensemble des applications et des sources de données de l'entreprise, que ce soit dans les environnements sur site ou cloud hybrides. Pour atténuer ce risque, la ZTDR exige la segmentation de l'infrastructure de sauvegarde en plusieurs zones de résilience ou domaines de sécurité (p. ex. le logiciel de sauvegarde, le stockage de sauvegarde principal et le stockage de sauvegarde secondaire), chaque zone bénéficiant d'un accès de moindre privilège, d'une surface d'attaque réduite et d'un rayon d'action minimal en cas d'attaque. Dans ce scénario, il se peut qu'une partie de la surface d'attaque du logiciel de sauvegarde reste exposée, mais celle du stockage de sauvegarde sera réduite au minimum. Pour ce faire, on utilise un contrôle d'accès Zero Trust et un protocole de communication sécurisé tel que S3 sur HTTPS afin de minimiser le risque de pénétration dans le composant de stockage de sauvegarde (voir **Figure 1**).

Figure 1

Architecture ZTDR (Zero Trust Data Resilience)

Séparation du logiciel et du stockage de sauvegarde



*to the BIOS, OS, the storage application, or data

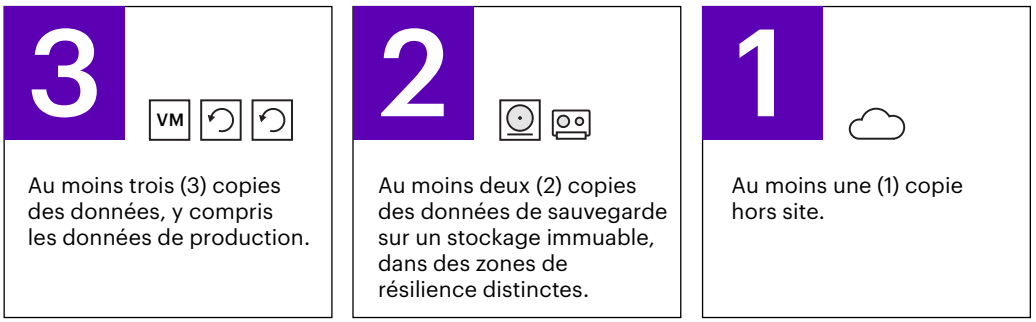
Plusieurs zones de résilience des données

La microsegmentation, qui consiste à diviser les périmètres de sécurité en zones plus réduites, fait partie des concepts fondamentaux du Zero Trust pour la gestion réseau. Elle permet d'assurer l'accès de moindre privilège, de réduire l'étendue des effets lorsqu'une zone est infectée, et de restreindre la mobilité latérale

des cybercriminels. Pour la 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.

Cette séparation crée une ligne de démarcation critique qui garantit la survie des données de sauvegarde, même lorsqu'un logiciel de sauvegarde est compromis. Cela peut se produire pour diverses raisons, y compris des acteurs internes malveillants. Tout système de sauvegarde doit garantir la restauration simple et rapide des données de sauvegarde à partir d'une installation propre du logiciel de sauvegarde. En créant plusieurs zones de résilience des données, vous garantissez l'efficacité de votre stratégie de sécurité multicouche et votre conformité à la règle de sauvegarde 3-2-1.

Règle de sauvegarde 3-2-1



Stockage de sauvegarde immuable

Conformément à la ZTDR, les données sauvegardées doivent également être immuables, de façon à empêcher toute modification ou suppression des données sauvegardées, même en cas d'attaque par ransomware. Pour maximiser la résilience des données, on peut fournir aux clients une cible de stockage renforcée et immuable, réglée en mode conformité avec **zéro accès au système d'exploitation ou au compte root**. Ce stockage peut inclure des solutions et des protocoles spécifiques au fournisseur ou des protocoles standard comme S3.

Immuabilité et sécurité S3-native

S3 offre l'immuabilité de stockage, la sécurité, l'IAM et le protocole de communication sécurisé les plus fiables du secteur.

Conception et architecture ouvertes

La conception et l'architecture ouvertes font partie des principes fondamentaux de la sécurité informatique en général. Pour respecter ce principe, il est préférable d'utiliser le protocole S3 de référence plutôt qu'un protocole propriétaire.

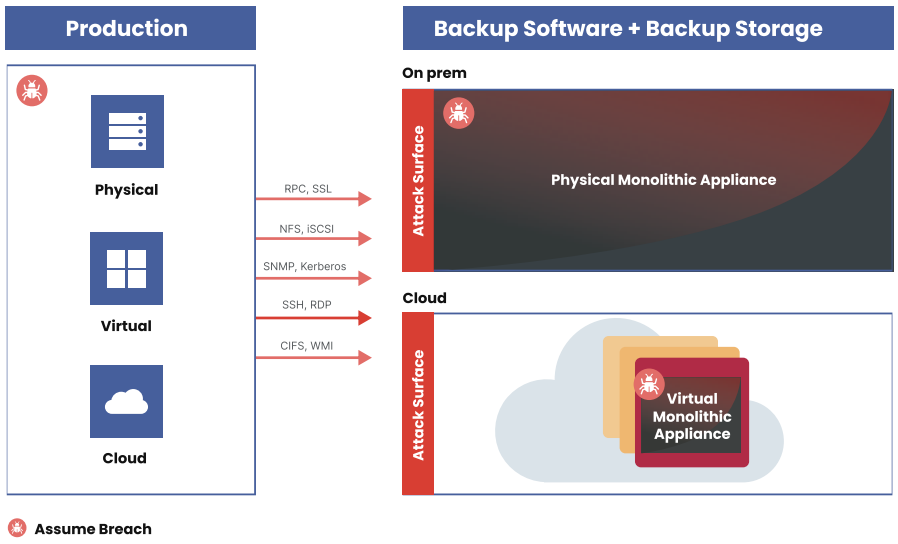
La segmentation entre les couches du logiciel de gestion des sauvegardes et du stockage des sauvegardes est une composante essentielle d'un système de sauvegarde et de restauration des données d'entreprise bien conçu. Cette segmentation est indispensable pour garantir la résilience, l'immuabilité et la flexibilité dont les entreprises ont besoin. Elle restreint en effet la surface d'attaque et garantit une sécurité multicouche, ce qui réduit considérablement le risque de corruption des données.

Appliance monolithique : Pas de Zero Trust

Les autres architectures comme les appliances monolithiques ne répondent pas aux exigences de la ZTDR, car elles n'assurent pas la séparation entre le logiciel et le stockage des sauvegardes. Cette architecture n'offre pas de véritable immuabilité, car, en cas d'intrusion, tout attaquant pourra accéder à l'intégralité du logiciel et du stockage. Il pourra alors modifier, supprimer ou rendre inaccessibles les données de sauvegarde. En d'autres termes, les effets de l'attaque toucheront l'ensemble du système de sauvegarde et de restauration (voir **Figure 2**). Cette approche implique également une grande confiance envers l'immuabilité du système de fichiers propriétaire du fournisseur.

Figura 2

Appliance monolithique. Sur site et dans le cloud. Pas de Zero Trust



- **Présumer l'existence d'une intrusion**
  dans une appliance physique ou une instance cloud
- **Pas de véritable immuabilité**
  n cas d'intrusion
- **Pas de séparation**
  du logiciel et du stockage de sauvegarde
- **L'attaque affecte l'intégralité de l'appliance**

En outre, il est important de comprendre que le déploiement d'une appliance virtuelle monolithique dans une instance cloud ne permet pas de garantir une véritable immuabilité dans le cadre d'un scénario cloud hybride. En cas de violation, lorsque des identifiants d'OS, d'instance ou de compte sont compromis, l'ensemble de l'appliance virtuelle devient vulnérable, ce qui étend les effets de la menace. La vulnérabilité provient de la sauvegarde des données sur le stockage propriétaire hébergé dans l'appliance virtuelle cloud. Pour résoudre ce problème (dû à un décalage architectural avec la ZTDR), on peut par exemple sauvegarder les données directement vers un stockage objet immuable dans le cloud, hors de l'instance.

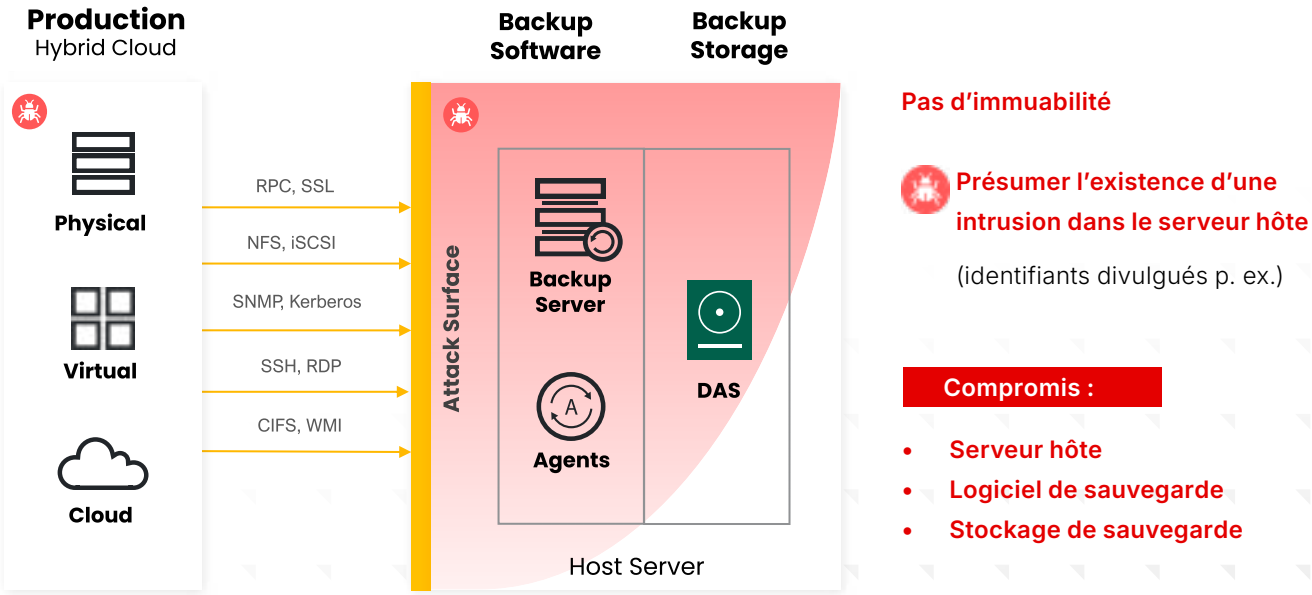
Direct-Attached Storage (DAS) : Pas de Zero Trust

Le Direct-Attached Storage (DAS, ou stockage en attachement direct) n'assure pas l'immuabilité : il est attaché directement au serveur Veeam Backup & Replication sans séparation entre le logiciel et le stockage de sauvegarde. Si un attaquant accède à l'hôte en exploitant une vulnérabilité OS ou applicative, il pourra accéder à toutes les données de ce système (voir **Figure 3**).

Figure 3

DAS — Direct-Attached Storage

PAS de Zero Trust. Pas de séparation du logiciel et du stockage de sauvegarde.



Conclusion

Face à la montée en puissance des cybermenaces, il est évident que les mesures de sécurité traditionnelles sont dépassées. Pour renforcer la cyberrésilience, il est essentiel d'adopter l'approche Zero Trust. Si les organisations appliquent de plus en plus les principes Zero Trust pour renforcer la protection de leurs données et limiter les interruptions de service, le Zero Trust Maturity Model (ZTMM) conventionnel n'offre pas de recommandations spécifiques pour la sauvegarde et la restauration des données d'entreprise.

La Zero Trust Data Resilience (ZTDR) est un nouveau modèle qui étend les principes Zero Trust à la sauvegarde et à la restauration des données. Ses principes fondamentaux : la segmentation du logiciel de sauvegarde et du stockage de sauvegarde, la création de plusieurs zones de résilience des données pour respecter la règle de sauvegarde 3-2-1, et un stockage de sauvegarde immuable pour protéger les données contre les modifications et les suppressions. Object First s'aligne sur ces meilleures pratiques pour offrir des solutions de stockage optimales afin de garantir une véritable résilience des données Zero Trust.

En adoptant la ZTDR, les organisations disposeront d'une approche claire et concrète pour renforcer leur posture de sécurité. Le résultat : des opérations plus efficaces et un meilleur alignement entre les équipes IT et sécurité, pour une reprise plus rapide et plus sûre.

Simply Resilient for Veeam

1.0_20251118

OBJECT FIRST