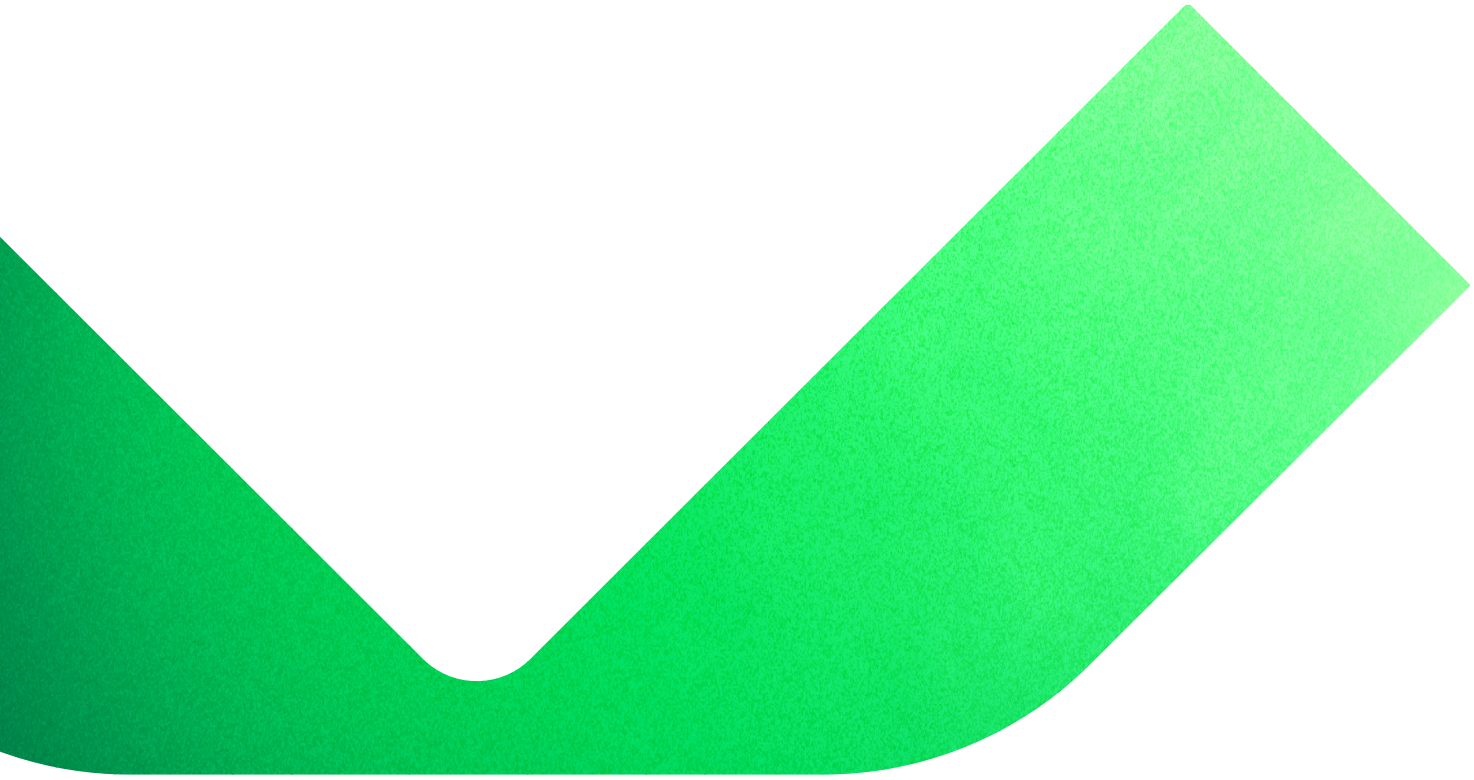
# Résilience des données Zero Trust

## Un modèle sécurisé de sauvegarde et de restauration des données



# Sommaire


| | |
|---|---|
| Résumé | 3 |
| Introduction | 4 |
| Approche | 5 |
| Résilience des données Zero Trust : Principes | 7 |
| Résilience des données Zero Trust : Architecture de référence | 12 |
| Résilience des données Zero Trust : Modèle de maturité étendu | 14 |
| Résumé du modèle de maturité | 19 |
| Conclusion | 19 |

# Résumé

Les grandes entreprises sont aujourd'hui confrontées à des défis importants pour protéger leurs données et leurs réseaux contre les acteurs malveillants, en particulier contre les ransomware et les attaques avec exfiltration de données. Pour répondre à ces préoccupations, une stratégie connue sous le nom de Zero Trust a gagné en popularité dans le secteur de la sécurité de l'information et est largement adoptée par les entreprises du monde entier.

Cependant, même les modèles Zero Trust les plus largement utilisés manquent de directives complètes dans certains domaines importants, en particulier en ce qui concerne la sauvegarde et la restauration des données. Conscients de l'importance de combler cette lacune et d'appliquer les principes Zero Trust dans ce domaine, nous introduisons le concept de résilience des données Zero Trust. Il s'agit d'un ensemble d'exigences, d'une architecture et d'une extension des modèles de maturité Zero Trust existants.

Plus précisément, les entreprises doivent utiliser un système de sauvegarde et de restauration qui leur garantit un stockage et une configuration inaltérables, tout en imposant un accès contextuel et fortement authentifié aux données sources en production et aux données sauvegardées. Ce système doit aussi prendre en charge de manière transparente les architectures hybrides courantes dans les entreprises d'aujourd'hui et gérer de manière flexible la restauration vers des environnements dissemblables.

En mettant en œuvre une architecture Zero Trust qui répond à ces exigences, les entreprises protégeront mieux leurs données, leurs réseaux et leurs applications contre les acteurs malveillants. Il est démontré que le Zero Trust offre une sécurité nettement supérieure à celle des approches traditionnelles, et les entreprises doivent l'adopter. Les nouvelles exigences de résilience des données proposées dans ce livre blanc renforcent et étendent le Zero Trust, et devraient être considérées comme obligatoires dans le cadre de la stratégie de sécurité de toute entreprise.

# Introduction

Le Zero Trust est une stratégie de sécurité et, par nécessité, sa portée est vaste. Cependant, les modèles et infrastructures Zero Trust dont l'utilisation est généralisée n'incluent pas tout[1]. Cela peut conduire à des lacunes ou à des omissions correspondantes dans les architectures de sécurité des entreprises. Plus spécifiquement, les systèmes de sauvegarde et restauration des données ne sont pas compris dans les infrastructures Zero Trust couramment utilisées. Cet écart est regrettable, car les données des entreprises sont très souvent la cible principale des acteurs malveillants, à la fois dans les ransomwares et dans les attaques d'exfiltration de données.

Les systèmes de sauvegarde et de restauration des données sont des éléments critiques de l'informatique d'entreprise et doivent être traités comme tels. Ils ont un accès en lecture à tous les éléments importants pour pouvoir les sauvegarder. Ils doivent également pouvoir écrire des données dans les environnements de production pour assurer leur fonction de restauration des données. Ils contiennent également une copie complète des données les plus importantes de l'entreprise. L'ensemble de ces attributs souligne l'importance des systèmes de sauvegarde et de restauration des données et met en évidence leur valeur en tant que cible pour les acteurs malveillants.

Bien sûr, les systèmes de sauvegarde et restauration des données relèvent de la responsabilité du service informatique depuis des décennies, mais n'ont souvent pas été inclus dans le périmètre ou la responsabilité des équipes de sécurité. Cependant, compte tenu de l'ampleur et de la sophistication des menaces de sécurité auxquelles les entreprises sont actuellement confrontées, adopter le seul point de vue de l'infrastructure réseau et IT pour la sauvegarde et la restauration des données ne suffit plus. Dans la pratique, nous avons rencontré des entreprises où ces systèmes étaient mal configurés et non supervisés, ce qui entraînait des risques importants.

Une sécurité moderne et efficace s'appuie sur les principes du Zero Trust. C'est pourquoi il est temps de porter un nouveau regard sur les systèmes de sauvegarde et de restauration des données. Ce livre blanc accomplit cela en proposant un nouveau concept de résilience des données Zero Trust. En adoptant cette approche, les entreprises disposeront d'une voie claire et concrète pour renforcer leurs défenses, améliorer l'efficacité de leurs opérations et accélérer leur restauration.

[1] Le document ZTMM de la CISA indique : « Bien que le ZTMM couvre de nombreux aspects de la cybersécurité essentiels pour les entreprises fédérales, il n'aborde pas d'autres aspects de la cybersécurité tels que… la restauration ».

# Approche

Les fondamentaux classiques de la sécurité de l'information, la triade CID : confidentialité, intégrité et disponibilité, sont tous applicables à la sauvegarde et à la restauration des données. Les entreprises doivent éviter l'exfiltration des données (confidentialité), empêcher les ransomwares de chiffrer les données (intégrité) et s'assurer que les systèmes sont à la fois protégés contre les attaques et peuvent être rapidement restaurés après une attaque (disponibilité).

Les principes fondamentaux du Zero Trust sont certainement pertinents dans ce domaine et doivent être appliqués aux accès système des utilisateurs et des systèmes informatiques de l'entreprise, ainsi qu'aux systèmes de sauvegarde et de restauration des données. Ces principes comprennent l'élimination de la confiance implicite et des réseaux non segmentés, le contrôle de tous les accès par des stratégies dynamiques et contextuelles via des points d'application des stratégies (PEP), l'exigence d'une authentification forte appropriée de tous les sujets, l'hypothèse d'une violation et la garantie et la validation de l'intégrité du système et des données. Dans ce livre blanc, nous verrons comment ces principes s'appliquent au nouvel ensemble d'exigences proposé pour une architecture de résilience des données Zero Trust.

L'infrastructure standard de facto pour examiner la maturité Zero Trust est le modèle de maturité Zero Trust de la CISA[2] illustré à la figure 1, qui définit cinq piliers fondamentaux : Identité, Appareils, Réseaux, Applications et Workloads, et Données. Il définit également trois capacités transversales : visibilité et analyses, automatisation et orchestration, et gouvernance.

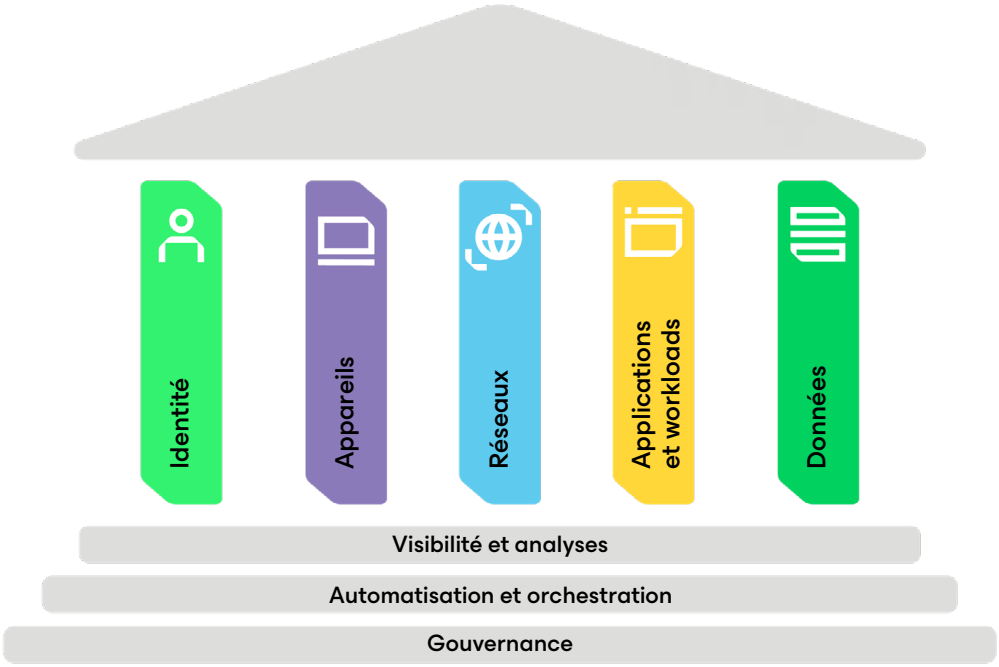



Figure 1 : Modèle de maturité Zero Trust de la CISA

[2] https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

À l'intérieur du pilier Données, le modèle CISA identifie cinq fonctions détaillées, avec des capacités et des attributs attendus pour chaque niveau de maturité.

Toutefois, au sein de ces fonctions, le sujet de l'intégrité de la sauvegarde des données et de la restauration est minime, et la CISA renvoie les lecteurs à un document du NIST de 2020 qui n'est pas lié au Zero Trust. En résumé, le modèle Zero Trust de la CISA ne spécifie pas les exigences et les niveaux de maturité des systèmes de sauvegarde et de restauration des données. Étant donné l'importance de ce domaine pour la confidentialité, l'intégrité et la disponibilité de l'entreprise, nous pensons que cette lacune doit être comblée.

Pour ce faire, nous introduisons le concept de résilience des données Zero Trust, qui comprend des principes, une architecture de référence et un nouvel ensemble de fonctionnalités pour le modèle de maturité Zero Trust. Pris ensemble, ils représentent une extension et une amélioration du Zero Trust, et se traduiront par une position de sécurité plus forte de l'entreprise.

**Les fonctions sont les suivantes :**


Gestion de l'inventaire des données


Catégorisation des données


Disponibilité des données


Accès aux données


Chiffrement des données

# Résilience des données Zero Trust : Principes

Les principes fondamentaux de la résilience des données Zero Trust sont :

**Moindre privilège** | **Inaltérabilité** | **Résilience du système** | **Validation proactive** | **Simplicité opérationnelle**

Discutons de chacun d'entre eux l'un après l'autre.

## Moindre privilège

Ce principe est au cœur du Zero Trust et doit faire partie de toute architecture Zero Trust. Cependant, cela vaut la peine d'examiner son applicabilité aux spécificités du ZTDR, car il s'applique à plusieurs niveaux. Du point de vue du réseau, le système de gestion des sauvegardes lui-même doit être isolé du réseau afin qu'aucun utilisateur ou périphérique non authentifié ou non autorisé ne puisse y accéder. De même, le système de stockage de sauvegarde doit être isolé. Cela empêche les acteurs malveillants de découvrir l'un ou l'autre de ces systèmes grâce à la reconnaissance du réseau ou à l'exploitation d'une vulnérabilité.

L'accès légitime et autorisé au système de sauvegarde doit se faire uniquement par le biais d'un point d'application de stratégie (PEP) Zero Trust avec une authentification forte et des vérifications de l'état des périphériques appropriées. Le PEP Zero Trust doit également contrôler l'accès aux données sources (c'est-à-dire les données sauvegardées), avec une authentification appropriée et un certain niveau de validation de l'appareil ou du système pour s'assurer que c'est le système de gestion des sauvegardes qui lit les données de production, et non un système ou un processus malveillant.

L'accès du système de gestion de sauvegarde au stockage de sauvegarde doit également être contrôlé par un PEP et séparé du reste du réseau au moyen d'une authentification forte appropriée. Notez que nous reviendrons sur cette exigence dans le diagramme d'architecture ci-dessous, car elle est importante : le système de stockage de sauvegarde doit être séparé du système de gestion des sauvegardes.

# Inaltérabilité

Le concept et l'exigence de données de sauvegarde inaltérables se sont généralisés ces dernières années, parallèlement à la prévalence et à la sophistication croissantes des ransomwares. Une sauvegarde inaltérable est définie comme étant des données sauvegardées au moyen d'un mécanisme de stockage qui, une fois écrit, ne peut plus être modifié. Le principe est le suivant : même si un acteur malveillant était présent sur le réseau et capable de prendre le contrôle du système de sauvegarde et d'accéder au stockage de sauvegarde, il serait dans l'incapacité de supprimer ou de modifier (chiffrer) les données sauvegardées. Une certaine inaltérabilité provient des propriétés physiques des supports de stockage, telles que les disques optiques WORM (écriture unique, lectures multiples), alors que les technologies plus récentes utilisent des supports dont l'inaltérabilité est appliquée au niveau du matériel, du micrologiciel ou des logiciels. Plus récemment, les principaux fournisseurs de services de cloud ont ajouté des fonctionnalités de stockage inaltérable pour répondre aux exigences de conformité et d'archivage des entreprises.

**REMARQUE**

Les exigences d'inaltérabilité s'étendent au-delà des données stockées et doivent également inclure des périodes de rétention des données. Certaines données inaltérables peuvent être configurées pour un stockage indéfini, alors que d'autres peuvent avoir une période de rétention définie (un à cinq ans, par exemple). En cas d'expiration du délai de rétention, les données peuvent être supprimées. Le système de stockage des données doit donc aussi assurer l'inaltérabilité de leur période de rétention. Cela évite les raccourcissements malveillants des périodes de rétention.

## Résilience du système

Nous avons une vision assez large de la résilience des systèmes et pensons qu'elle doit s'appliquer non seulement à l'infrastructure de sauvegarde elle-même, mais à l'ensemble de l'écosystème des outils, technologies et processus liés à la sauvegarde et à la restauration des données. Plus précisément, l'infrastructure de sauvegarde doit être résiliente aux défaillances et aux attaques telles que l'indisponibilité des composants ou du réseau, ou la manipulation du NTP (Network Time Protocol) afin de faire expirer les données sauvegardées de manière malveillante. Il doit également être facile de configurer l'utilisation de stockages de données de sauvegarde distribués et hétérogènes, par exemple à travers plusieurs zones géographiques ou types d'infrastructure. La résilience est également améliorée en séparant les données de sauvegarde du système de gestion des sauvegardes, afin que la compromission du système de sauvegarde n'entraîne pas également celle du stockage des données. En fait, optez pour un système de gestion des sauvegardes que vous pourrez reconstituer sans incidence sur votre capacité à accéder aux données sauvegardées et à les restaurer en cas de compromission ou de défaillance.

Le système doit également être résilient aux changements attendus et inattendus de l'environnement de l'entreprise. Les changements prévus incluent l'ajout ou la suppression planifiée de composants de l'infrastructure, y compris l'adoption d'applications et de données hybrides ou basées sur le cloud. Cela étant, le système de sauvegarde doit être capable de capturer et de stocker efficacement les données d'entreprise, indépendamment de leur emplacement source ou de leur technologie. Les changements inattendus se produisent généralement pendant la réponse aux incidents ou la reprise après incident (DR) et sont le plus souvent regroupés dans la catégorie du support pour la restauration dans des environnements différents. Lorsqu'une entreprise restaure des données, il est tout à fait possible que l'environnement de restauration s'exécute sur un autre site ou dans un autre type d'infrastructure. Par exemple, un datacenter local inondé peut nécessiter une restauration dans un environnement basé sur le cloud, avec des opérations qui s'y poursuivent pendant une période prolongée. Par conséquent, le système de sauvegarde doit prendre en charge à la fois la restauration dans cet environnement différent et les nouvelles sauvegardes depuis cet environnement de production.

En plus de fournir un stockage de données inaltérable, le système de stockage des données de sauvegarde doit pouvoir être renforcé facilement. Cela peut prendre la forme d'une appliance pré-renforcée ou d'un système configurable par l'administrateur avec des recommandations de renforcement claires, qui conviendra mieux à des entreprises sophistiquées.

## Validation proactive

Pour assurer le bon fonctionnement du système, il faut surveiller le système et valider tous ses aspects fonctionnels et ses processus. Cela comporte deux aspects. Tout d'abord, il convient de superviser le système de sauvegarde pour le réseau, la performance et la sécurité. C'est-à-dire que ce système doit être traité comme n'importe quel autre système de production à forte valeur ajoutée.

Deuxièmement, et c'est le plus important, la validité des données sauvegardées ainsi que la fiabilité et l'efficacité des processus de restauration doivent être régulièrement validées. Par définition, la restauration des données sauvegardées se produira à des moments inattendus, probablement dans un environnement très stressant. Il est important que l'entreprise dispose d'un processus bien compris, bien documenté et bien rodé. Il doit également y avoir plusieurs personnes capables d'effectuer cela pour tenir compte des vacances, de l'indisponibilité et du roulement du personnel.

Gardez à l'esprit que, bien que cela nécessite un investissement en temps et en énergie, cela démontre une maturité opérationnelle et constitue une « police d'assurance » en cas de catastrophe. Notez également que le terme « catastrophe » ne signifie pas nécessairement une catastrophe au sens littéral du terme ou un événement majeur tel qu'une inondation de datacenter. Par exemple, une entreprise avec laquelle nous avons travaillé a connu un flux de travail automatisé incontrôlé en raison d'une erreur de programmation, ce qui a entraîné la suppression d'importantes quantités de données de production dans son système de gestion financière. Ce n'était pas un désastre littéral, et cela n'a pas dégénéré en désastre figuratif en utilisant leurs processus (validés) de restauration des données.

En outre, le système de gestion des sauvegardes doit avoir la capacité directe ou indirecte d'organiser les sauvegardes selon la chronologie d'une infection par un logiciel malveillant. C'est-à-dire qu'il doit être capable de détecter les (ou d'être informé des) infections par des logiciels malveillants et de catégoriser les sauvegardes comme saines, douteuses ou compromises, selon le moment où elles ont été effectuées.

**REMARQUE**

Les processus de validation et de restauration des données doivent également respecter les exigences de confidentialité et de résidence des données. Cela peut augmenter la complexité et les risques, et il faut donc le faire de manière réfléchie, en connaissant à la fois le contenu des données et les obligations légales et de conformité de l'organisation.

## Simplicité opérationnelle

Notre dernier principe est la simplicité opérationnelle, que nous définissons comme un système suffisamment facile à utiliser pour que votre entreprise puisse l'utiliser en toute confiance, tout en offrant suffisamment de capacités, d'évolutivité et de sophistication pour répondre pleinement aux besoins de votre entreprise. C'est-à-dire un système adapté à votre organisation.

C'est important : nous avons vu des entreprises s'efforcer d'utiliser et de rendre opérationnels des systèmes trop complexes par rapport à la taille, à l'équipe, aux compétences et aux besoins de leur organisation. Il en résulte des avantages limités, de la frustration et une incapacité à fournir la maturité en matière de sécurité ou la valeur commerciale. L'une des caractéristiques à rechercher chez un fournisseur de sauvegarde est sa capacité relative en matière d'orchestration et d'automatisation. Les fournisseurs disposant de solides capacités dans leurs plateformes seront plus rapides et plus faciles à opérationnaliser.

Pour conclure cette section, chacun de ces principes est tissé dans les nouvelles extensions du modèle de maturité dont il est question plus loin dans ce document, et sera également apparent dans l'architecture de référence dont nous parlerons ensuite.

# Résilience des données Zero Trust : Architecture de référence

Les architectures de sauvegarde des données varieront nécessairement d'une entreprise à l'autre, compte tenu de l'énorme variabilité des infrastructures réseau, d'application et de données, entre autres facteurs. Néanmoins, il existe des éléments architecturaux communs en raison des principes Zero Trust communs, qui doivent être présents dans toute architecture de résilience des données Zero Trust.

Notre architecture de référence (figure 2) illustre les principales exigences de ce type de système. Veuillez remarquer que cette description de l'environnement se place du point de vue du système de gestion des sauvegardes. L'accès régulier et quotidien des utilisateurs et des systèmes aux systèmes de production serait également contrôlé par des PEP Zero Trust, mais cela est omis dans le diagramme pour plus de clarté.

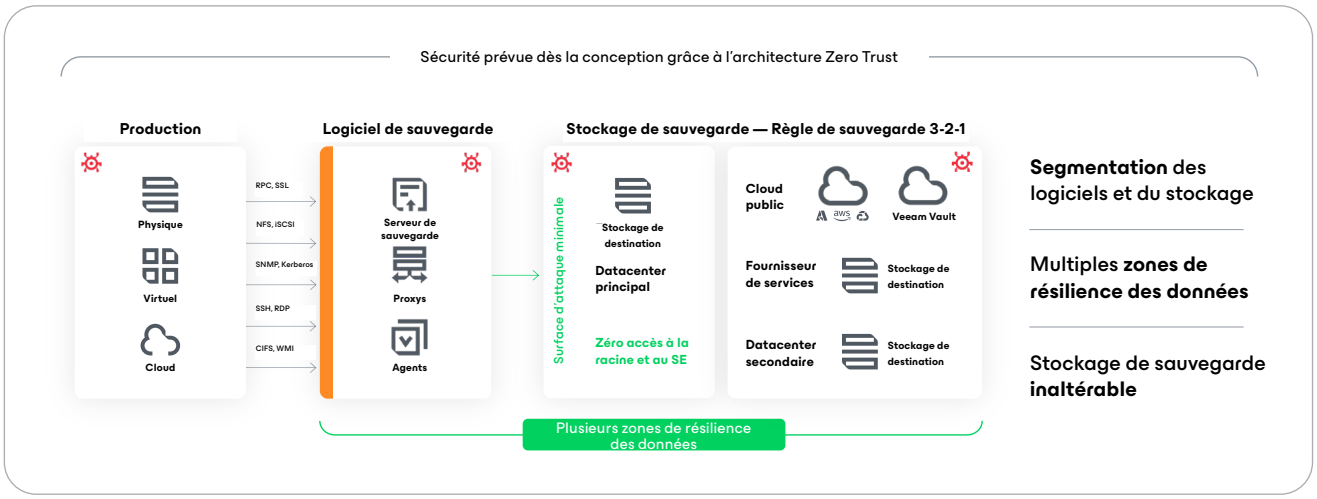



Figure 2 : Résilience des données Zero Trust : Architecture de référence

Tout d'abord, notez les éléments essentiels de toute architecture Zero Trust : le point de décision de stratégie (PDP) centralisé, qui délègue l'authentification de l'identité au système de gestion des identités et des accès (IAM) de l'entreprise. Le PDP s'appuie sur son ensemble de stratégies pour prendre des décisions d'accès pour les identités authentifiées, y compris les identités humaines et non humaines (système). Dans cette architecture, le PDP prend les décisions d'accès au système de gestion des sauvegardes. Ces décisions sont communiquées par l'intermédiaire du plan de contrôle (représenté par des lignes pointillées) avec les points d'application des stratégies (PEP) qui s'intercalent logiquement entre le système de gestion des sauvegardes, les sources de données à sauvegarder et les emplacements de sauvegarde cibles.

L'architecture comprend également une structure recommandée pour les données sauvegardées. Outre l'exigence d'inaltérabilité des données, les entreprises doivent s'efforcer d'en conserver au moins une copie dans un emplacement principal disposant d'une connexion réseau à faible latence vers le site de restauration prévu. Cela permet d'obtenir des snapshots de sauvegarde rapides, ce qui favorise des points de restauration plus fréquents et des temps de restauration plus courts. Bien sûr, l'emplacement principal est souvent commun avec celui des systèmes de production. Notre architecture de référence illustre donc également l'objectif de disposer d'au moins 2 copies des données dans des sites secondaires[3]. Ceux-ci doivent être isolés géographiquement de l'emplacement principal pour assurer la résilience en cas de catastrophe régionale. Le compromis probable est une connexion réseau plus lente, ce qui peut se traduire par des points de restauration moins fréquents et des temps de restauration plus longs.

**REMARQUE**

Le système de gestion de la sauvegarde est volontairement séparé de ses catégories de stockage. Le système de sauvegarde assure ainsi une répartition transparente des données sauvegardées entre plusieurs cibles inaltérables et géographiquement réparties. Cela permet aussi aux grandes entreprises de choisir les cibles de stockage de sauvegarde qui offrent la meilleure combinaison de performances, de prix et de simplicité opérationnelle pour leurs besoins spécifiques. Il fournit également une couche de sécurité supplémentaire en contrôlant la communication via un PEP.

[3] Il existe plusieurs écoles de pensée à propos du nombre de sauvegardes dans divers emplacements, souvent désignées par des moyens mnémotechniques tels que 3-2-1 ou 3-2-1-1-0.

# Résilience des données Zero Trust : Modèle de maturité étendu

Bien que les principes et l'architecture de référence que nous avons proposés pour la résilience des données Zero Trust soient universellement applicables, ils ne peuvent pas être pleinement et immédiatement appliqués à la plupart des entreprises. En ce qui concerne la plupart des aspects du Zero Trust, ils doivent être planifiés et adoptés progressivement. La façon standard de modéliser et de communiquer cela est d'utiliser un modèle de maturité. Comme nous l'avons mentionné dans l'introduction, nous suivons l'infrastructure standard de facto du modèle de maturité Zero Trust de la CISA et l'étendons avec quatre nouvelles fonctions qui constituent nos principes et nos exigences.

Ces nouvelles fonctions sont les suivantes :

**Accès aux données et systèmes de l'entreprise**

**Accès au stockage et aux données de sauvegarde**

**Résilience du système**

**Supervision et validation du système**

Ces extensions ZTDR du modèle de maturité sont illustrées dans les figures 3 à 6, qui montrent comment chacune des quatre nouvelles fonctions devrait être avancée à travers les niveaux de maturité habituels : Traditionnel, Initial, Avancé et Optimal.

Pour chacune des fonctions, nous avons identifié des attributs attendus pour chaque niveau de maturité. Le modèle décrit ainsi les améliorations et les changements qu'une organisation doit apporter afin de progresser en maturité pour chaque fonction. Ensuite, nous examinons successivement chacune des fonctions au fur et à mesure qu'elle progresse dans les niveaux de maturité.

# Accès aux données et systèmes de l'entreprise

Cette fonction est définie comme étant l'ensemble des moyens et mécanismes par lesquels le système de gestion des sauvegardes (BMS) a accès aux données sources qu'il est chargé de sauvegarder.

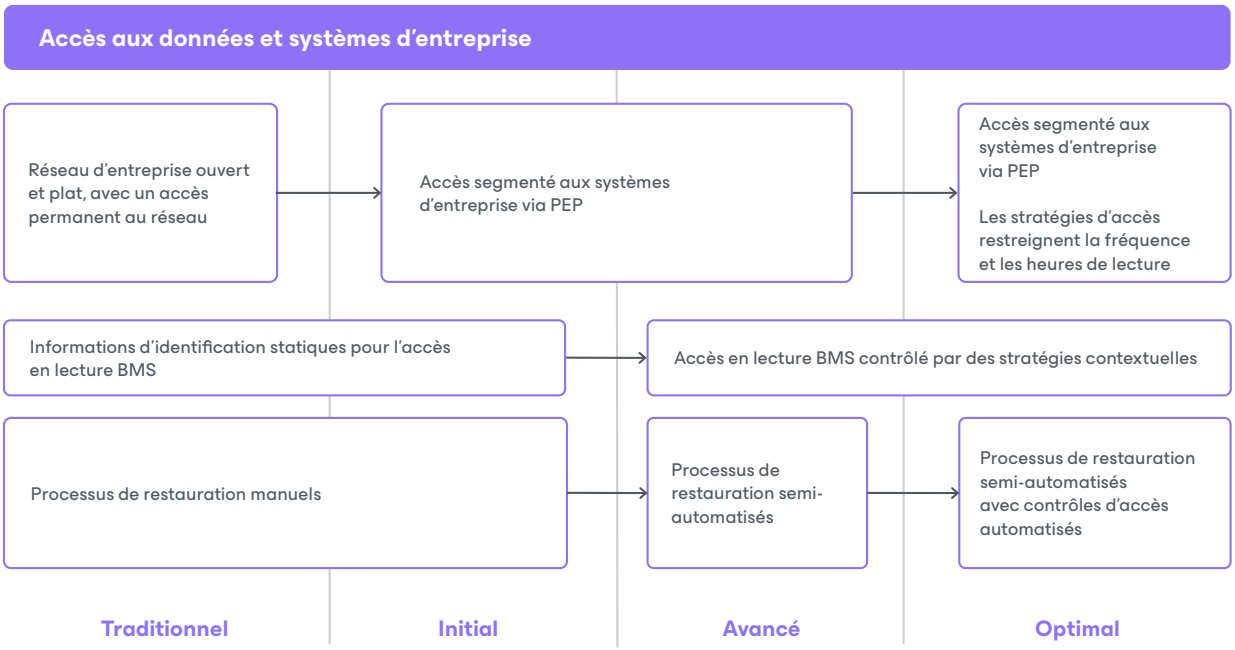



Figure 3 — Accès aux données et systèmes de l'entreprise : Modèle de maturité

Au niveau de maturité **traditionnel**, l'entreprise dispose d'un réseau plat et ouvert, et le système de gestion des sauvegardes dispose d'un accès réseau continu et sans entrave aux systèmes sources. Le BMS utilise des informations d'identification statiques, telles qu'une clé API, un nom d'utilisateur/mot de passe stocké ou un certificat, afin d'authentifier et de lire les données sources. Lorsque l'entreprise utilise le BMS pour restaurer un système, elle s'appuie sur des processus manuels.

Afin de passer au niveau **initial**, l'entreprise doit commencer à appliquer une meilleure segmentation du réseau et restreindre l'accès BMS aux systèmes d'entreprise via un point d'application de stratégie Zero Trust, introduisant le principe du moindre privilège.

Lorsque l'entreprise est au niveau **avancé**, elle a introduit des stratégies d'accès contextuel pour l'accès BMS aux données et aux systèmes de l'entreprise, ce qui permet de mieux utiliser les fonctionnalités dynamiques d'application des stratégies Zero Trust. Ils ont aussi commencé à utiliser des processus de restauration automatisés avec quelques étapes manuelles pour lancer et valider le processus.

Au niveau **optimal**, l'entreprise a amélioré son utilisation des stratégies d'accès, afin de limiter l'accès BMS aux seules périodes autorisées ou aux événements de restauration active. Cela renforce le principe du moindre privilège.

# Accès au stockage et aux données de sauvegarde

Cette fonction est définie comme étant les moyens et mécanismes par lesquels le système de gestion des sauvegardes dispose d'un accès en écriture et en lecture au stockage de sauvegarde et aux données qui y sont stockées.

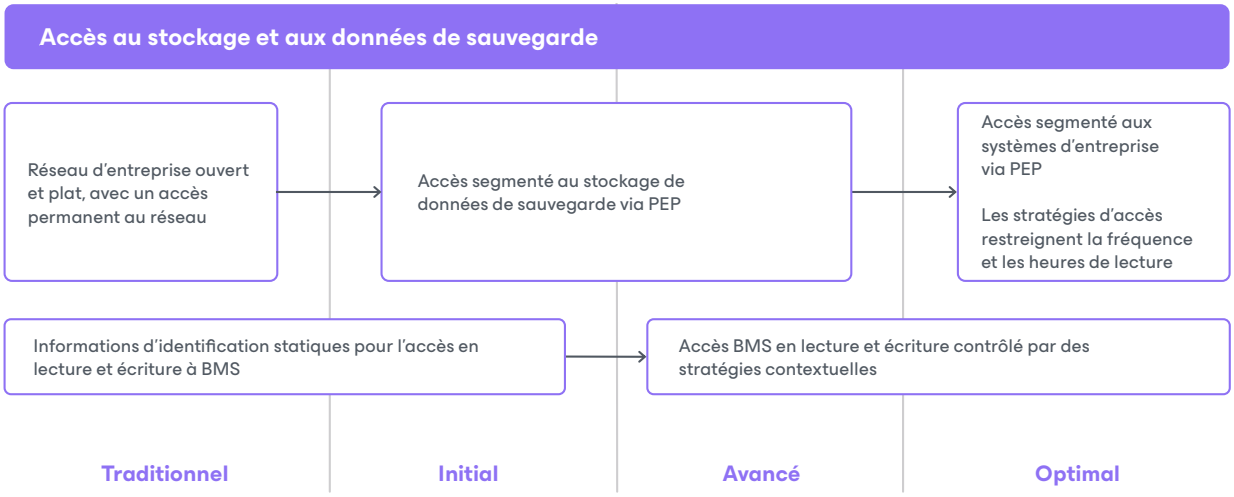



Figure 4 — Accès au stockage de sauvegarde et aux données : Modèle de maturité

Au niveau de maturité **traditionnel**, l'entreprise dispose d'un réseau plat et ouvert, et le système de gestion des sauvegardes dispose d'un accès réseau continu et sans entrave au système de stockage des sauvegardes et aux données sauvegardées qui y sont stockées. Le BMS utilise des informations d'identification statiques, telles qu'une clé API, un nom d'utilisateur/mot de passe stocké ou un certificat, afin d'authentifier et d'écrire sur le stockage, et de lire les données stockées.

Afin de passer au niveau **initial**, l'entreprise doit commencer à appliquer une meilleure segmentation du réseau et à restreindre l'accès BMS au stockage de sauvegarde et aux données stockées au moyen d'un point d'application de stratégie Zero Trust afin d'appliquer le principe du moindre privilège.

Lorsque l'entreprise atteint le niveau **avancé**, elle a introduit des stratégies d'accès contextuel pour l'accès BMS au système de stockage de sauvegarde et aux données stockées. Cela permet de mieux utiliser les fonctionnalités dynamiques d'application des stratégies au sein de l'entreprise.

Au niveau **optimal**, l'entreprise a amélioré son utilisation des stratégies d'accès, afin de limiter l'accès BMS au stockage aux seules périodes autorisées ou pendant les événements de restauration active. Cela renforce le principe du moindre privilège.

# Résilience du système

Cette fonction est définie comme étant les caractéristiques du système de sauvegarde en ce qui concerne sa résistance aux pannes système, aux défaillances de composants ou aux activités malveillantes.

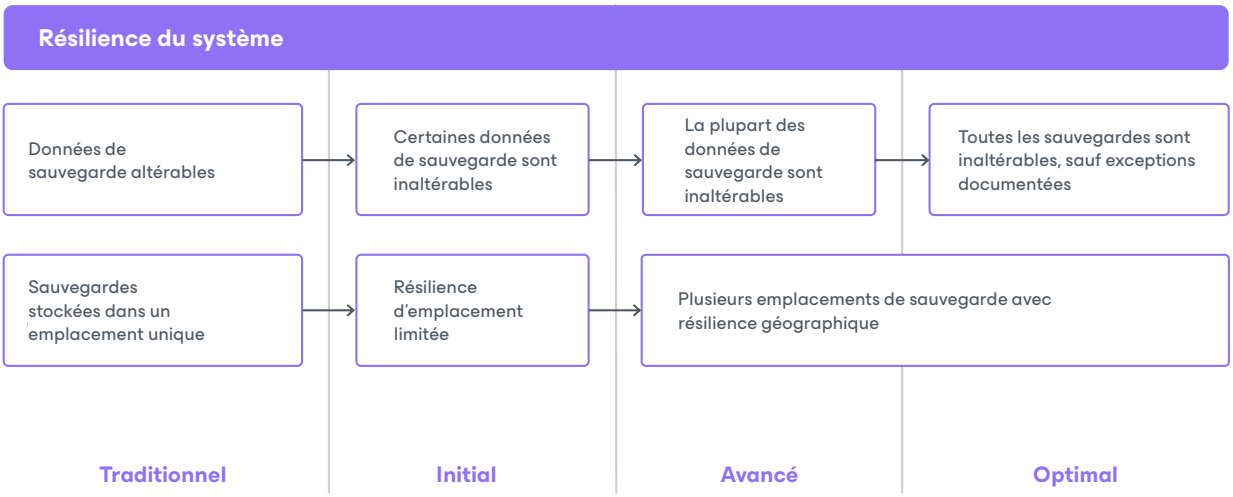



Figure 5 — Résilience du système : Modèle de maturité

Au niveau de maturité **traditionnel**, l'entreprise utilise un stockage mutable pour les données de sauvegarde, ce qui met en danger l'intégrité et la disponibilité de celles-ci. En outre, elles stockent généralement les sauvegardes dans un seul emplacement, exposant ainsi l'entreprise à des pertes totales en cas de catastrophe régionale.

En passant au niveau **initial**, l'entreprise doit commencer à utiliser un stockage inaltérable pour certaines de ses sauvegardes de données et introduire une résilience d'emplacement limitée pour ces sauvegardes.

Au niveau **avancé**, l'entreprise utilise principalement un stockage de sauvegarde inaltérable, idéalement basé sur la sensibilité et la criticité des données. Ils ont aussi introduit et opérationnalisé l'utilisation de multiples emplacements de stockage de sauvegarde répartis géographiquement.

Lorsque l'entreprise a atteint le niveau **optimal**, elle utilise pleinement le stockage de sauvegarde inaltérable, avec toutes les exceptions documentées et approuvées. Les nouvelles sources de données et applications utiliseront par défaut une sauvegarde inaltérable. Ce niveau offre à l'entreprise une résilience maximale contre les sinistres régionaux et les acteurs malveillants.

# Supervision et validation du système

Il s'agit des outils et processus qui permettent à l'entreprise de s'assurer que son système de gestion des sauvegardes et son stockage de sauvegarde fonctionnent correctement et qu'elle est capable d'exécuter un processus de restauration lorsque nécessaire.

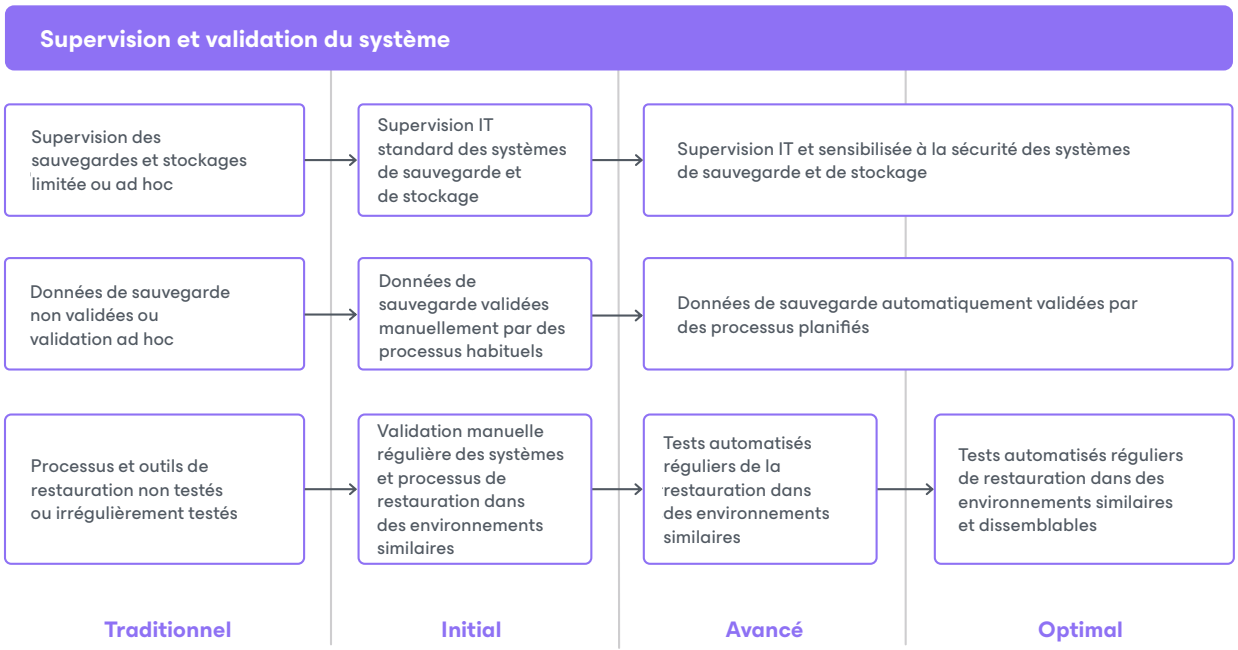



Figure 6 — Supervision et validation du système : Modèle de maturité

Au niveau de maturité **traditionnel**, l'entreprise n'effectue que la supervision de base de l'infrastructure de sauvegarde et de stockage, ce qui reflète souvent un degré de maturité global inférieur de l'informatique et de l'exploitation. Il est possible que l'entreprise ne vérifie pas les données sauvegardées ou n'effectue que des vérifications occasionnelles (c.-à-d. manuelles et peu fréquentes). De plus, l'entreprise ne teste pas régulièrement les outils et les processus de restauration pour qu'ils soient bien compris, documentés et reproductibles.

Au niveau **initial**, ils ont adopté un niveau standardisé de supervision IT et opérationnelle du système de sauvegarde et de stockage. Ils mettent aussi en place une validation régulière des données sauvegardées au moyen de processus manuels. Ils ont également mis en place une validation régulière (manuelle) des processus de restauration afin de s'assurer de leur connaissance institutionnelle et de leur familiarisation.

Au niveau **avancé**, les entreprises ont déployé des outils et des processus de supervision IT et de la sécurité pour leurs systèmes de sauvegarde et de stockage. De plus, ils valident automatiquement les données sauvegardées grâce à des vérifications planifiées qui signalent et font remonter tout résultat anormal. Cela comprend des tests automatisés des outils et des processus de restauration dans des environnements similaires à ceux de production.

Au niveau **optimal**, l'entreprise a amélioré ses tests de restauration pour les tester dans des environnements dissemblables.

# Résumé du modèle de maturité

Prises dans leur ensemble, ces nouvelles fonctions définissent un ensemble de fonctionnalités et un ensemble de compétences attendues, mises en correspondance avec les quatre niveaux de maturité Zero Trust. Elles fournissent une feuille de route et un guide pratique aux entreprises qui souhaitent intégrer leurs systèmes de sauvegarde et de restauration des données dans leur initiative Zero Trust.

# Conclusion

Le Zero Trust est manifestement une meilleure façon d'aborder la sécurité de l'information, et en tant que leaders de la sécurité, nous avons l'obligation d'appliquer cette stratégie dans nos entreprises. Les architectures et les modèles de maturité Zero Trust actuels sont des points de départ solides, mais sont incomplets. En particulier, les exigences et approches en matière de sauvegarde et de restauration des données en sont absentes.

Jusqu'à présent, les grandes entreprises considéraient la sauvegarde et la restauration comme relevant du domaine de l'IT, mais la prévalence des ransomwares et la numérisation quasi complète de l'activité obligent les responsables de la sécurité à élargir leur champ d'action.

Dans ce livre blanc, nous avons introduit le concept de résilience des données Zero Trust, avec un ensemble de principes fondamentaux, une architecture de référence et des extensions du modèle de maturité Zero Trust. Nous pensons qu'en adoptant cette approche de résilience des données Zero Trust, les entreprises disposeront d'une voie claire et concrète vers des défenses plus solides, des opérations plus efficaces et une restauration plus rapide. Les données d'entreprise sont trop importantes pour que nous n'appliquions pas les meilleures pratiques de sécurité, et le Zero Trust est le moyen le plus efficace de le faire.

### À propos de Veeam Software

Veeam®, le n° 1 mondial de la résilience des données, estime que chaque entreprise doit pouvoir se relever après un incident en conservant la confiance et le contrôle de toutes ses données, au moment et à l'endroit voulus. Veeam appelle cela la résilience totale, et nous sommes obsédés par le désir de créer des moyens innovants d'aider nos clients à y parvenir. Les solutions Veeam sont spécifiquement conçues pour renforcer la résilience des données en offrant la sauvegarde, la restauration, la liberté des données, la sécurité des données et l'intelligence des données. Avec Veeam, les responsables IT et de la sécurité ont la tranquillité d'esprit de savoir que leurs applications et leurs données sont protégées et toujours disponibles dans l'ensemble de leurs environnements cloud, virtuels, physiques, SaaS et Kubernetes. Basé à Seattle et possédant des bureaux dans plus de 30 pays, Veeam protège plus de 550 000 clients dans le monde, dont 74 % des entreprises du Global 2000, qui lui font confiance pour le maintien de leur activité. La résilience totale commence avec Veeam. Pour en savoir plus, rendez-vous sur www.veeam.com ou suivez Veeam sur LinkedIn @veeam-software et X @veeam.

**En savoir plus : veeam.com**