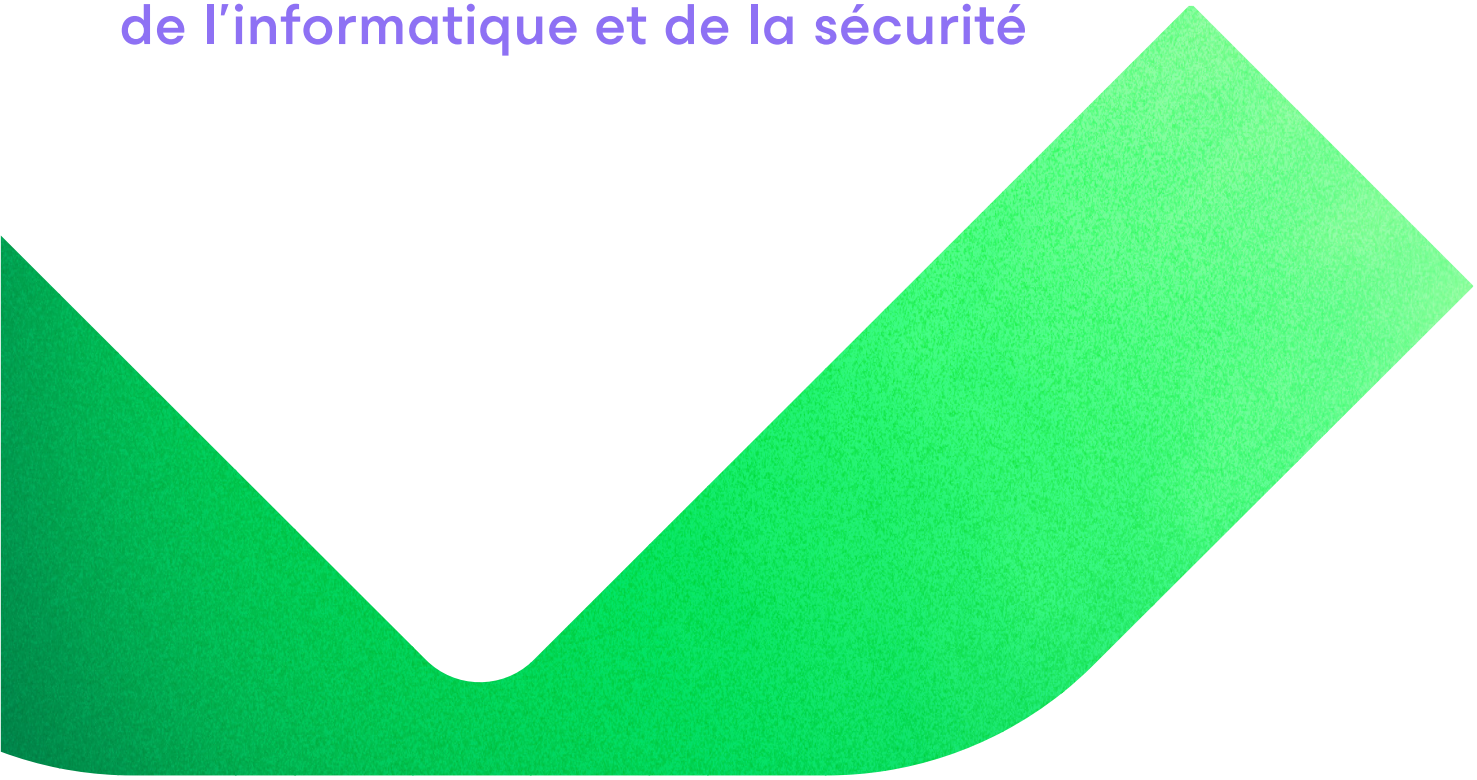
Étendre le Zero Trust à la sauvegarde et à la restauration des données

Guide pratique pour les professionnels de l'informatique et de la sécurité



Sommaire

Résumé

Le Zero Trust est une stratégie moderne et très efficace pour mieux sécuriser l'infrastructure informatique de notre entreprise contre les ransomwares et autres menaces. Les systèmes de sauvegarde et de restauration des données sont essentiels pour nos entreprises et doivent être inclus dans toute initiative Zero Trust.

Cependant, le Zero Trust peut être compliqué à concevoir et à mettre en œuvre, et jusqu'à présent, il n'existait aucun consensus sur la meilleure manière de l'appliquer aux systèmes de sauvegarde et de restauration des données.

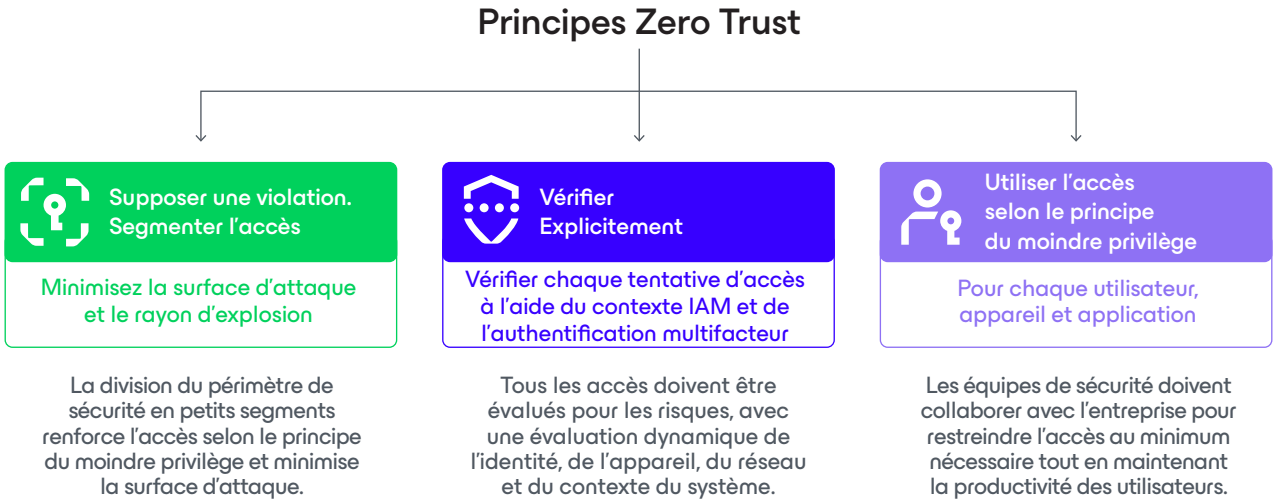
Le nouveau modèle de résilience des données Zero Trust (ZTDR) introduit par Veeam et Numberline Security s'appuie sur le modèle de maturité Zero Trust de la Cybersecurity and Infrastructure Security Agency (CISA). Le ZTDR étend les principes de Zero Trust à la sauvegarde et à la restauration, garantissant ainsi aux entreprises la possibilité de réduire les risques et d'atteindre leurs objectifs de sécurité et de résilience.

En suivant l'approche de résilience des données Zero Trust expliquée dans ce guide, vous découvrirez ce que vous devez rechercher dans une plateforme et une architecture de sauvegarde et de restauration des données, et vous serez en mesure de démarrer rapidement et efficacement dans votre environnement.

Zero Trust : Une brève introduction

Le Zero Trust est une stratégie de sécurité moderne basée sur l'idée qu'aucun utilisateur, appareil ou paquet réseau ne doit être considéré implicitement comme digne de confiance. Pour garantir la sécurité des données, l'accès aux actifs de données stratégiques doit être segmenté et toutes les communications doivent être authentifiées, évaluées et autorisées avant tout accès. Celle-ci doit s'appliquer à chaque segment et à ses données, applications, actifs ou services.

Il s'agit d'un changement significatif par rapport aux architectures traditionnelles de sécurité de l'information, qui s'appuyaient sur des périmètres statiques basés sur le réseau, et qui ont clairement échoué à protéger nos entreprises contre les ransomwares et les acteurs malveillants.



Présentation de la résilience des données Zero Trust (ZTDR)

Les systèmes de sauvegarde et de restauration des données sont des éléments cruciaux de l'informatique d'entreprise et des cibles fréquentes des attaques. Ils doivent être sécurisés de manière adéquate et globalement.

En suivant les principes du ZTDR et en choisissant les fournisseurs de sauvegarde et de stockage selon les conseils du ZTDR, votre entreprise bénéficiera d'une meilleure défense, d'une exploitation plus efficace et d'une restauration plus rapide et plus fiable.

ZTDR étend les principes fondamentaux du Zero Trust

EXIGENCES DE LA SOLUTION

Séparation du logiciel de sauvegarde et du stockage de sauvegarde

Minimisez la surface d'attaque et le rayon d'explosion

Choisissez des solutions de sauvegarde et de restauration des données dont l'architecture établit une séparation entre le logiciel de sauvegarde et le stockage, et qui, idéalement, empêche l'accès root ou SE au stockage de sauvegarde.

Ces fonctionnalités vous permettront d'appliquer strictement les contrôles d'accès via des politiques Zero Trust.

Plusieurs Zones de résilience

Règle de sauvegarde 3-2-1

Recherchez des solutions de sauvegarde et de restauration des données qui prennent en charge plusieurs zones de résilience. Cela signifie que votre entreprise peut survivre à la perte ou à la compromission d'un seul système de sauvegarde ou environnement de stockage.

Vous pourrez ainsi respecter facilement la règle du 3-2-1 en matière de sauvegarde.

Inaltérable Stockage de sauvegarde

Protéger les données de sauvegarde contre toute modification ou suppression

Optez pour des solutions de sauvegarde et de restauration qui prennent en charge facilement et efficacement un stockage de sauvegarde inaltérable et fiable.

Vous avez ainsi la certitude que vos données sauvegardées sont protégées contre toute suppression ou modification, même en présence d'un acteur malveillant.

La règle du 3-2-1 pour les meilleures pratiques de sauvegarde :

3

3 copies des données, y compris les données de production.

2

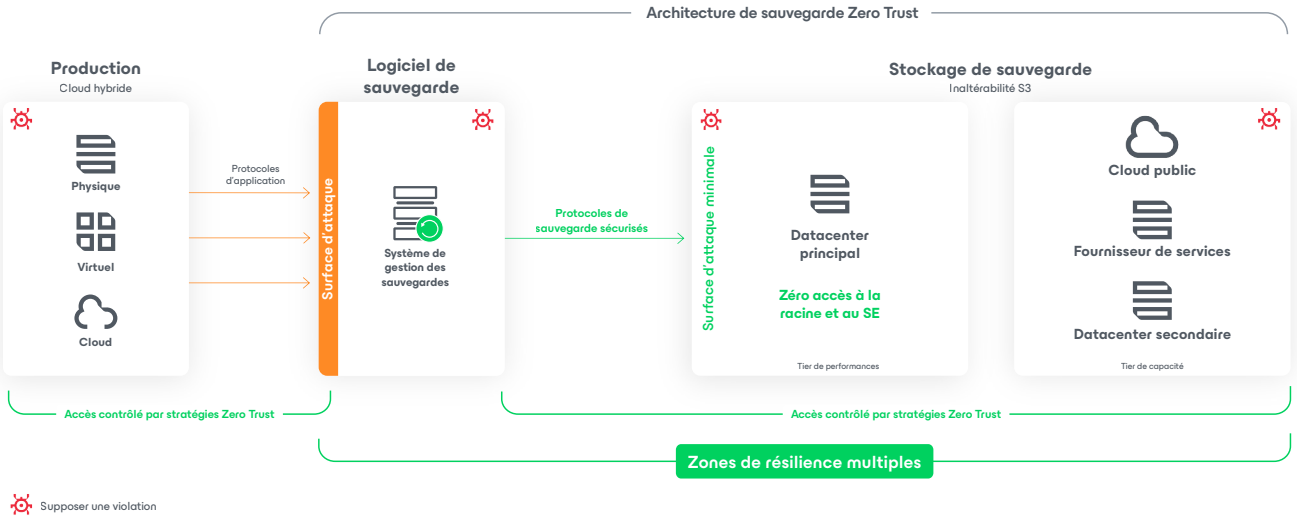
2 copies des données de sauvegarde sur un stockage inaltérable dans des zones de résilience distinctes

1

1 copie hors site.

Architecture de référence ZTDR

L'architecture de référence ZTDR vous montre comment déployer une plateforme Zero Trust en conjonction avec vos systèmes de gestion et de stockage des sauvegardes.



Prise en main du ZTDR

Bien que le Zero Trust soit une démarche, il existe des mesures immédiates et efficaces que vous pouvez prendre pour améliorer la résilience de sécurité de votre infrastructure de sauvegarde et de restauration des données.

Cette semaine :

Découvrez dans quelle mesure vos systèmes de sauvegarde et de restauration répondent aux exigences ZTDR.

Tâche	Questions à poser
Discuter de la segmentation de votre réseau avec vos équipes d'infrastructure réseau et IT	• Comment notre réseau est-il segmenté ? • Le logiciel et le stockage de sauvegarde sont-ils segmentés en zones de sécurité distinctes ? • Comment l'accès à chaque segment de l'infrastructure de sauvegarde est-il contrôlé ?
Évaluer si le stockage de vos données de sauvegarde est organisé en plusieurs zones de résilience	• Suivons-nous les directives du secteur en matière de 3-2-1 ? • Qu'advient-il de nos processus de sauvegarde et de restauration si une de nos zones de sauvegarde n'est pas disponible ? • Qu'advient-il de nos processus de sauvegarde et de restauration si deux de nos zones de sauvegarde ne sont pas disponibles ?
Vérifier si vos systèmes de stockage de sauvegarde sont correctement inaltérables	• Comment votre fournisseur de stockage documente-t-il et garantit-il l'inaltérabilité ? • Un administrateur malveillant peut-il modifier les paramètres d'inaltérabilité ou de rétention au moyen d'un accès root ou SE au stockage ? • Que se passe-t-il si le temps système est avancé de manière malveillante ?
Valider vos processus de restauration	• Quel est notre plan de reprise après incident ? Quand l'avons-nous testé pour la dernière fois ? • Combien de personnes de l'équipe informatique ou de stockage peuvent restaurer un système en suivant les étapes documentées ? • Que se passe-t-il si (personne importante X) n'est pas disponible lors d'un incident ?

La semaine prochaine :

Validez vos processus et vos outils, puis planifiez et parvenez à un consensus sur les modifications à court et moyen terme de votre infrastructure et de vos processus de sauvegarde et de restauration.

Tâche	Questions à poser
Évaluer votre confiance et la répétabilité de vos processus de restauration en effectuant des tests réguliers (hebdomadaires/mensuels)	• À quelle fréquence effectuons-nous les tests de restauration ? • Qu'avons-nous appris au sujet de la documentation ou des lacunes dans les processus ? • Quand pouvons-nous y remédier ?

Tâche	Questions à poser
Commencer à planifier la configuration du réseau, la segmentation ou les changements de règles de pare-feu	• Avec qui, au sein de l'équipe informatique ou de sécurité, puis-je collaborer pour évaluer l'étendue des changements potentiels ? • Qui, au sein de l'équipe de sécurité, dirige notre initiative Zero Trust et comment puis-je la soutenir ? • Quels sont les changements de segmentation du réseau ou d'infrastructure en cours ?
Planifier tout changement de configuration du stockage ou évaluation par de nouveaux fournisseurs afin de combler tout écart d'inaltérabilité	• Quel est notre processus d'évaluation et d'acquisition de stockage de sauvegarde supplémentaire ? • Quel type de justification financière, d'efficience ou de risque devrions-nous faire ? • Comment dois-je procéder pour obtenir l'approbation nécessaire au lancement d'un processus d'évaluation des fournisseurs ?
Désigner des responsables pour les améliorations des processus et de la documentation	• Qui serait impliqué dans l'approbation et la mise en œuvre des changements apportés au (processus X) ? • Comment pouvons-nous fixer un délai d'implémentation mutuellement acceptable ?

Le mois prochain :

Commencez à implémenter des changements à court terme et commencez à identifier les changements nécessaires à long terme.

Tâche	Questions à poser
Déployer vos processus de reprise après incident améliorés et testez à nouveau	• Dans quelle mesure nos processus de DR se sont-ils améliorés ? • Avons-nous comblé toutes les lacunes en matière de processus et de documentation ?
Valider et itérer sur la segmentation du réseau	• Quelles sont les zones du réseau qui autorisent encore un large accès réseau vers et depuis nos systèmes de sauvegarde ? • Comment renforcer cela pour améliorer notre résilience face aux ransomwares ?
Réaliser des améliorations sur la capacité de stockage, les emplacements et l'inaltérabilité	• Quel est notre degré de satisfaction par rapport à notre capacité de stockage de sauvegarde ? • Quel est notre degré de confiance dans l'inaltérabilité de nos systèmes de stockage de sauvegarde ? • Respectons-nous les directives des meilleures pratiques du 3-2-1 ? • Comment utilisons-nous plusieurs zones de résilience ?

Que devez-vous rechercher d'autre ?

Validation proactive de la reprise après incident

Les incidents nécessitant la restauration des données sauvegardées vont se produire à des moments inattendus, probablement dans des circonstances très stressantes. Il est important que votre entreprise dispose de plans et de processus de reprise d'activité bien compris, bien documentés et bien répétés. Assurez-vous également d'avoir un degré élevé de confiance dans l'intégrité et la validité des données sauvegardées.

Simplicité opérationnelle

Assurez-vous de choisir un système suffisamment simple pour que votre entreprise puisse l'utiliser facilement et en toute confiance, tout en offrant suffisamment de capacités, d'évolutivité et de sophistication pour répondre pleinement aux besoins de votre entreprise. Efforcez-vous de bien comprendre les capacités et les compétences de votre personnel, afin que les opérations ne dépendent pas d'une seule personne ou d'un seul « superhéros ».

Foire aux questions

Le Zero Trust est-il quelque chose que vous pouvez acheter auprès d'un fournisseur ?

Non, le Zero Trust est quelque chose que vous **faites** : c'est une stratégie de sécurité qui change et améliore l'informatique, la sécurité et les résultats commerciaux.

Le Zero Trust se contente-t-il de restreindre l'accès et de réduire la productivité des utilisateurs ?

Non, le Zero Trust consiste à éliminer tous les accès **inutiles**, tout en maintenant la productivité des utilisateurs. De nombreuses entreprises **améliorent** réellement la productivité et l'expérience utilisateur grâce au Zero Trust.

Pourquoi le Zero Trust est-il important ?

Le Zero Trust est le moyen le plus efficace de défendre nos entreprises contre des risques tels que les ransomwares, les acteurs malveillants et d'autres risques. Compte tenu du paysage actuel des menaces, il est de notre responsabilité de l'utiliser.

Pouvez-vous utiliser votre infrastructure de sécurité actuelle pour le Zero Trust ?

Très probablement, oui ! Lorsqu'ils sont utilisés correctement, les systèmes modernes de pare-feu, d'identité et d'infrastructure peuvent vous aider à entamer votre parcours Zero Trust. Atteindre des niveaux optimaux de maturité Zero Trust peut nécessiter des investissements supplémentaires, qui peuvent être guidés par des outils tels que l'architecture de référence ZTDR.

Ressourcessupplémentaires

Vous voulez en savoir plus sur le Zero Trust et le ZTDR ?

- Visitez le site Web de Veeam pour lire l'étude ZTDR complète et découvrir l'approche de Veeam en matière de sécurité des données et de cyber-résilience.
- Pour lire l'intégralité du livre blanc de recherche sur le ZTDR et pour obtenir le point de vue de Numberline Security à ce sujet, visitez le site Web de Numberline.

À propos de Veeam Software

Veeam, le n° 1 mondial de la résilience des données, estime que les entreprises doivent contrôler toutes leurs données à tout instant et à l'endroit où elles en ont besoin. Veeam assure la résilience des données en couvrant divers aspects essentiels tels que la sauvegarde, la restauration, la libre circulation, la sécurité et l'analyse intelligente des données. Basé à Seattle, Veeam protège plus de 550 000 clients dans le monde entier qui lui font confiance pour le maintien de leur activité. Pour en savoir plus, rendez-vous sur www.veeam.com/fr ou suivez Veeam sur LinkedIn @veeam-software et X @veeam.

En savoir plus : veeam.com