



CHECKLIST IMPRIMABLE

Rançongiciel : validez votre vraie capacité de restauration

Une sauvegarde immuable peut préserver un point de restauration fiable, mais elle ne protège pas à elle seule tout le système d'information. Utilisez cette checklist pour vérifier si votre dispositif résisterait réellement à une attaque et permettrait de redémarrer.

Au sommaire

- 1 À retenir avant de commencer
- 2 Vérifier la protection des copies
- 3 Contrôler les accès et l'administration
- 4 Quel mécanisme apporte quelle protection ?
- 5 Tester la restauration avant l'incident
- 6 Verdict à inscrire dans votre plan de reprise

À retenir avant de commencer

L'immutabilité empêche la modification, la suppression ou l'écrasement d'une copie pendant une durée de rétention définie.

L'efficacité dépend de copies antérieures à l'attaque, de droits séparés, d'une isolation suffisante et de restaurations réellement testées.

Elle protège l'intégrité d'une copie, mais ne bloque ni l'intrusion ni le chiffrement des systèmes de production.

Une restauration complète doit inclure les données, les applications, les bases de données, les annuaires, les certificats et les configurations nécessaires.

COMPARATIF DES MÉCANISMES DE PROTECTION DES SAUVEGARDES			
Aucun mécanisme n'est universel : combinez-les pour une résilience maximale.			
MÉCANISME	ACCESSIBILITÉ	FORCE	LIMITE
 SAUVEGARDE IMMUABLE	 Accessible au système autorisé	 Empêche la modification pendant la rétention	 Dépend de la configuration et des comptes d'administration
 SAUVEGARDE HORS LIGNE	 Non accessible en permanence	 Réduit l'exposition aux attaques réseau	 Restauration et exploitation moins immédiates
 COPIE DÉCONNECTÉE	 Isolée du réseau selon le dispositif	 Limite les accès directs depuis la production	 Demande une organisation et des contrôles physiques ou logiques
 RÉPLICATION	 Souvent accessible rapidement	 Accélère la disponibilité d'une autre copie	 Peut reproduire des données chiffrées ou corrompues
 BONNES PRATIQUES  Appliquez la règle 3-2-1-1-0 pour diversifier et sécuriser vos sauvegardes.  Testez régulièrement vos restaurations pour valider leur efficacité.  Surveillez et auditez en continu vos dispositifs de sauvegarde.  Documentez et formez vos équipes aux procédures de reprise.			

INFOGRAPHIE Comparatif des sauvegardes immuables, hors ligne, déconnectées et répliquées contre les rançongiciels.

Vérifier la protection des copies

Les sauvegardes sont verrouillées contre la modification, la suppression et l'écrasement. Vérifiez le mécanisme d'immutabilité et la durée de rétention réellement appliquée.

- Plusieurs points de restauration sains sont conservés.**
Ne dépendez pas d'une copie unique susceptible d'être postérieure ou déjà contaminée.
- La rétention couvre la période nécessaire à la détection de l'incident.**
Une copie ne protège que pendant la durée où elle reste disponible et fiable.
- Les copies protégées sont antérieures à une éventuelle compromission.**
Contrôlez l'historique et recherchez des signes de chiffrement ou de corruption.
- Une copie est placée sur un emplacement distinct.**
Réduisez le risque de compromission simultanée des environnements.
- Une copie isolée ou déconnectée complète le dispositif lorsque cela est possible.**
L'isolement limite les accès directs depuis la production.

Contrôler les accès et l'administration

- Les comptes de production et les comptes d'administration des sauvegardes sont distincts.**
Une compromission de la production ne doit pas donner automatiquement les mêmes privilèges sur les sauvegardes.
- Les droits d'accès au stockage et à la console sont limités au strict nécessaire.**
Réduisez la portée d'un compte compromis.
- L'authentification multifacteur est activée pour les accès sensibles.**
Portez une attention particulière aux comptes privilégiés.
- Le verrouillage des copies ne peut pas être retiré depuis un poste de production compromis.**
Examinez la séparation et l'indépendance des contrôles d'administration.
- La configuration du stockage et la gestion des clés sont régulièrement revues.**
L'immutabilité dépend aussi de ces paramètres et des droits accordés.

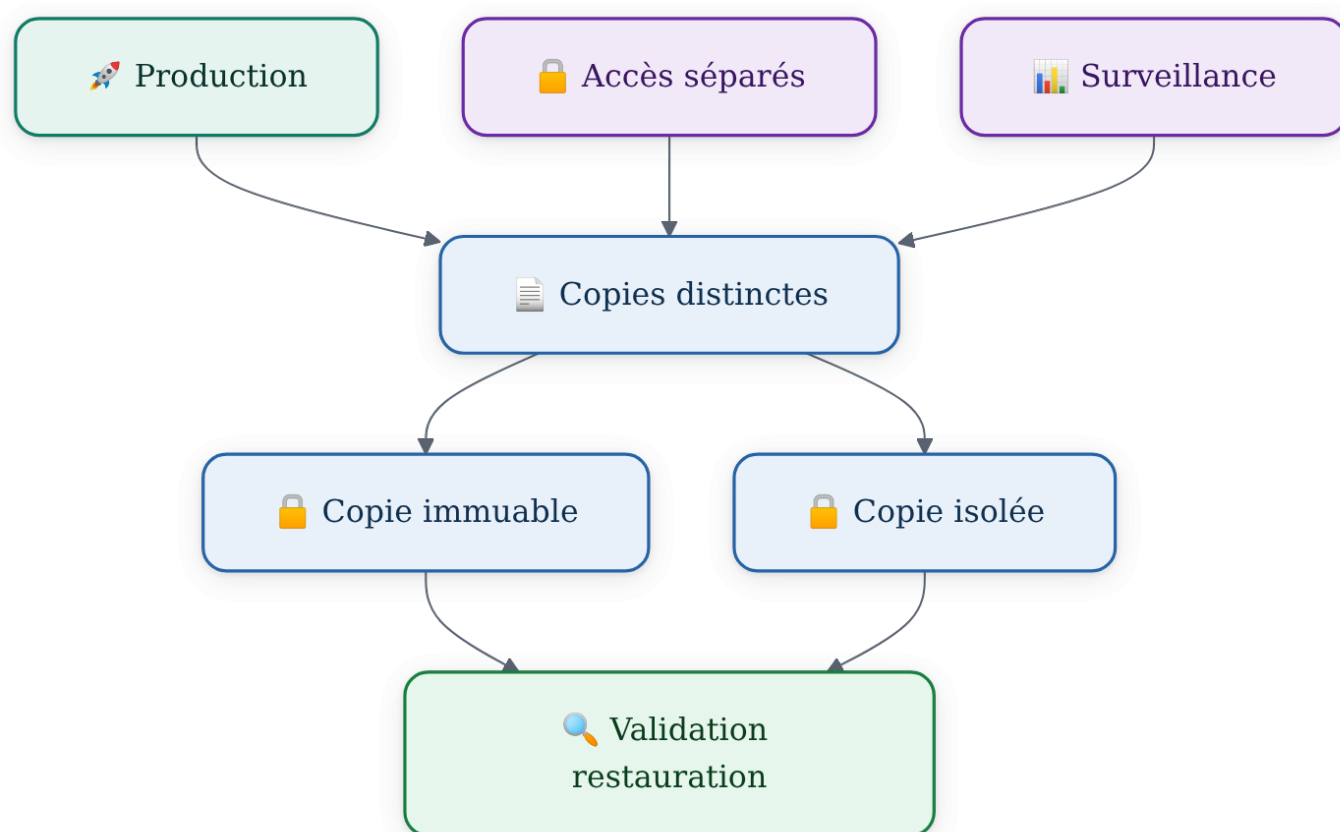
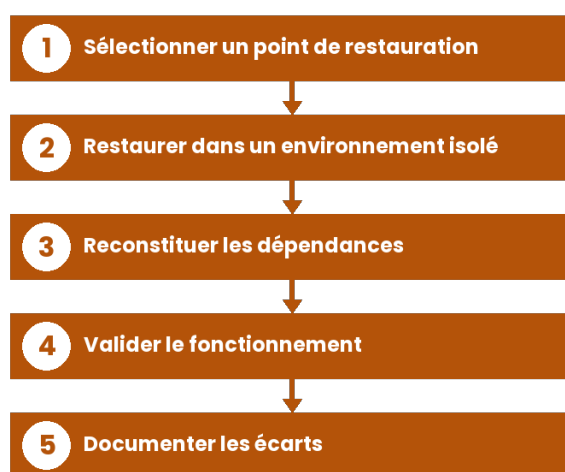


SCHÉMA Combiner plusieurs copies, une sauvegarde immuable et une copie isolée pour limiter le risque de perte simultanée.

Quel mécanisme apporte quelle protection ?

Mécanisme	Force principale	Point de vigilance
Sauvegarde immuable	Empêche la modification pendant la rétention	Dépend de la configuration et des comptes d'administration
Sauvegarde hors ligne	Réduit l'exposition aux attaques réseau	Accès et restauration moins immédiats
Copie déconnectée	Limite les accès directs depuis la production	Demande une organisation et des contrôles adaptés
Réplication	Met rapidement une autre copie à disposition	Peut reproduire des données chiffrées ou corrompues

Tester la restauration avant l'incident



1 Sélectionner un point de restauration

Choisissez une copie antérieure à l'incident supposé et vérifiez qu'elle n'est ni chiffrée ni corrompue.

2 Restaurer dans un environnement isolé

Évitez de tester directement dans la production afin de ne pas propager une compromission ou une corruption.

3 Reconstituer les dépendances

Incluez les applications, bases de données, annuaires, certificats, configurations et autres éléments nécessaires au redémarrage.

4 Valider le fonctionnement

Contrôlez que les données sont exploitables et que les services essentiels peuvent réellement redémarrer.

5 Documenter les écarts

Notez les éléments manquants, les droits nécessaires et les étapes à corriger avant de considérer le plan de reprise comme opérationnel.

! Ne pas confondre copie intacte et reprise réussie

Une sauvegarde immuable peut rester intacte tout en étant insuffisante pour redémarrer l'activité. La restauration doit être testée avec l'ensemble des composants et dépendances nécessaires.

Verdict à inscrire dans votre plan de reprise

Considérez la sauvegarde immuable comme un filet de sécurité, pas comme une défense complète contre les rançongiciels. Elle doit s'inscrire dans une stratégie combinant séparation des accès, segmentation, détection, copies distinctes et tests réguliers de restauration.

À adapter à votre architecture, à vos exigences de reprise et à votre politique de sécurité. Une copie immuable ne remplace pas les autres mesures de protection.