Sauvegarde cyber-résiliente des serveurs dans le Cloud

pour les ETI, PME et organismes publics

Livre Blanc

Sommaire

Introduction 3
Le risque ransomware : pourquoi vos sauvegardes sont la cible 4
La sauvegarde, une problématique pour les PME, ETI et collectivités 5
La règle d'or de la sauvegarde : du 3-2-1 au 3-2-1-1-0 5
La sauvegarde des serveurs dans le Cloud 6
Modes de sauvegarde : fichiers et image de volume 6
La déduplication à la source : la bande passante maîtrisée 7
Un moteur open source : Restic, la transparence 7
L'immutabilité des sauvegardes 8
Le chiffrement de bout en bout 8
La résistance post-quantique contre les menaces de demain 10
Restauration : la seule métrique qui compte le jour J 10
Le chargement initial des données dans le Cloud 12
Hébergement européen, droit européen, zéro transfert hors UE 12
L'orchestrateur Cybee : l'industrialisation de la sauvegarde 14
La Console Cybee : piloter et superviser en toute autonomie 14
Trois scénarios d'utilisation typiques 15
Les bénéfices de la sauvegarde Cloud cyber-résiliente 15
Questions fréquentes 16
Conclusion 17

Introduction

Selon les études les plus récentes, entre **23 % et 46 %** des organisations ne testent jamais la restauration de leurs sauvegardes [1], et à peine la moitié testent leur plan de reprise d'activité au moins une fois par an [3]. Plus préoccupant encore : lors des tests, seuls **58 %** des serveurs ont pu être restaurés dans les délais prévus par les SLA et dans **42 %** des cas, les données se sont révélées inaccessibles ou inexploitables au moment critique [2]. Ces négligences conduisent à des situations graves : perte définitive de données, indisponibilité prolongée du système d'information, voire cessation d'activité.

Les ransomwares (ou rançongiciels) représentent aujourd'hui la menace numéro un pour les entreprises et les administrations. Ils sont devenus la principale source d'inquiétude pour les DSI, les RSSI et leurs dirigeants, car les attaques modernes ne se limitent plus au chiffrement des données de production : elles ciblent délibérément les sauvegardes pour empêcher toute restauration et maximiser la pression sur la victime.

Selon les études sectorielles récentes, la grande majorité des attaques par ransomware comportent une tentative de compromission des sauvegardes (une étude de Sophos en 2024 montre qu'**environ 94%** des attaques par ransomware comportent une **tentative de compromission des sauvegardes).**

Lorsque les sauvegardes sont corrompues, l'entreprise victime n'a souvent plus d'autre choix que de payer la rançon, et ce sans aucune garantie de récupération.

Face à cette évolution, les messages traditionnels (« externalisez vos sauvegardes ») sont devenus insuffisants. La cyber-résilience exige désormais trois propriétés que ce livre blanc développe en détail : **l'étanchéité** (l'attaquant qui contrôle votre SI ne doit pas pouvoir atteindre vos sauvegardes), **l'immutabilité** (une sauvegarde écrite ne peut être ni modifiée ni supprimée pendant sa durée de rétention) et **la vérifiabilité** (une sauvegarde n'a de valeur que si sa restauration est testée).

Ce livre blanc, rédigé par les équipes de **Cybee**, éditeur français de sauvegarde Cloud, donne aux responsables informatiques de PME, d'ETI et d'organismes publics les clés pour bâtir une stratégie de sauvegarde capable de résister aux cyberattaques actuelles et à celles de demain, y compris la menace quantique.

Le risque ransomware : pourquoi vos sauvegardes sont la cible

Depuis plusieurs années, les attaques par ransomware visant les entreprises et les institutions ont dépassé en nombre celles touchant les particuliers. L'ANSSI a documenté la professionnalisation de groupes cybercriminels qui ciblent spécifiquement des organisations financièrement solvables, dans le cadre d'attaques dites « Big Game Hunting », dont la sophistication rivalise parfois avec des opérations d'espionnage étatique.

Le mode opératoire a évolué : l'attaquant s'introduit dans le système d'information, y demeure plusieurs heures ou jours, utilise l'IA, cartographie l'infrastructure, **y compris les serveurs et consoles de sauvegarde**, puis déclenche le chiffrement simultané des données de production et des sauvegardes. La double extorsion (chiffrement + menace de divulgation des données exfiltrées) est devenue la norme.

Exemple de cas client

Une ETI sauvegardait ses machines virtuelles avec un logiciel leader du marché. Les sauvegardes étaient conservées en local et répliquées, via un partage, vers un second datacenter. L'attaquant, présent dans le SI depuis l'été, a lancé son ransomware : les fichiers, les sauvegardes locales et les sauvegardes distantes ont été chiffrés en une seule opération.

L'attaque a réussi parce que les espaces de stockage des sauvegardes restaient **connectés en permanence** au système d'information, avec les mêmes technologies et les mêmes identifiants. Résultat : dix jours de blocage complet et le paiement d'une partie de la rançon pour récupérer les données critiques. Dans d'autres cas documentés, c'est le catalogue local des sauvegardes qui a été chiffré, rendant inutilisables les supports externalisés.

Planifier sa cyber-résilience

Pour limiter la gravité d'une attaque, trois principes s'imposent :

1. **Rupture technologique** entre les données de production et le stockage des sauvegardes : l'attaquant qui a compromis l'infrastructure locale ne doit pas pouvoir accéder aux sauvegardes externalisées avec les mêmes outils, protocoles ou identifiants. Le stockage objet S3, avec ses mécanismes d'accès propres, constitue cette barrière.
2. **Catalogue des clichés et métadonnées hors d'atteinte** : la reconstruction des données doit rester possible même si le site principal est intégralement compromis. Avec un format de dépôt autoporteur comme celui de Cybee, le dépôt distant contient tout ce qui est nécessaire à la restauration.
3. **Immutabilité des sauvegardes externalisées** : même un attaquant disposant d'identifiants valides ne doit pas pouvoir supprimer ni modifier les sauvegardes pendant leur durée de rétention (verrouillage de type Object Lock, présenté plus loin).

La sauvegarde, une problématique pour les PME, ETI et collectivités

Certaines stratégies de sauvegarde des ETI, PME et collectivités reposent encore sur des sauvegardes sur site (on-premise), externalisées à intervalle plus ou moins régulier et rarement testées, faute de temps des équipes informatiques.

Les chiffres du marché confirment la fragilité de ces approches : selon Veeam, seuls 58 % des serveurs testés ont pu être restaurés dans les délais prévus par les SLA, et à peine **13 %** des entreprises disposent d'une orchestration automatisée de leur plan de reprise d'activité [2]. En parallèle, les ransomwares mettent sous pression les stratégies traditionnelles, y compris celles bâties sur les logiciels leaders du marché, dont les mécanismes sont précisément étudiés par les attaquants.

L'arrivée du Cloud et du stockage objet a changé la donne depuis 10 ans : des sauvegardes plus simples à opérer, moins coûteuses, dédupliquées pour économiser la bande passante et surtout plus faciles à vérifier. À condition de choisir une solution conçue pour la cyber-résilience et non un simple espace de stockage Cloud distant.

La règle d'or de la sauvegarde : du 3-2-1 au 3-2-1-1-0

La règle intemporelle du **3-2-1** reste le socle de toute stratégie de sauvegarde :

1. **3 copies** des données : le fichier source et deux sauvegardes ;
2. **2 supports** de technologies différentes et étanches entre elles ;
3. **1 copie externalisée**, hors du site principal.

Mais cette règle ne suffit plus face aux cybermenaces actuelles : des attaques ont permis de chiffrer à la fois les données, les sauvegardes locales et les sauvegardes externalisées, en rendant indisponible le catalogue ou en supprimant les données distantes. La règle moderne, recommandée par les acteurs de la cybersécurité, est le **3-2-1-1-0** :

- **1 copie immuable ou hors ligne** : une sauvegarde verrouillée en écriture (WORM / Object Lock), qu'aucun attaquant, ni aucun administrateur compromis, ne peut altérer pendant la durée de rétention ;
- **0 erreur de restauration** : des vérifications d'intégrité et des tests de restauration réguliers, car une sauvegarde non testée est une sauvegarde présumée défaillante.

L'exigence clé : l'étanchéité. Un attaquant ayant pris le contrôle de votre système d'information ne doit avoir aucun moyen d'accéder à vos sauvegardes externalisées, ni de les supprimer. C'est la rupture technologique (stockage objet, identifiants distincts, immutabilité) qui crée cette étanchéité, pas la simple distance géographique.

La sauvegarde des serveurs dans le Cloud

L'objectif de la sauvegarde des serveurs dans le Cloud est de sécuriser les données critiques de l'entreprise vers un centre de données externe, en s'affranchissant de la manipulation de cartouches et de bandes, et de leur externalisation physique.

Pour sauvegarder vers l'extérieur, il faut disposer d'un lien Internet dont le débit montant est suffisant : c'est un point clé. Un lien fibre de 50 Mbit/s ascendant permet d'envisager la sauvegarde de plusieurs dizaines de machines (physiques ou virtuelles) et de plusieurs téraoctets de données, d'autant plus aisément que la solution déduplique les données à la source, comme le fait Cybee (voir plus loin).

Les fonctionnalités attendues d'une sauvegarde en ligne moderne

- **Chiffrement de bout en bout** : les données sont chiffrées à la source, avant tout envoi, et le fournisseur n'a aucun accès en clair à leur contenu ;
- **Déduplication à la source** pour réduire drastiquement les volumes transmis et stockés ;
- **Gestion des versions** (clichés horodatés, règles de rétention, profondeur d'historique) ;
- **Immutabilité** du stockage pour résister aux ransomwares ;
- **Planification et orchestration** : fenêtres de sauvegarde, priorisation, maîtrise de la bande passante ;
- **Supervision** : rapports d'exécution, alertes automatiques par e-mail, vérification d'intégrité des dépôts ;
- **Réversibilité** : un format de stockage ouvert et documenté, exploitable sans dépendance à l'éditeur.

Modes de sauvegarde : fichiers et image de volume

La sauvegarde en mode fichiers

La sauvegarde en mode fichiers protège les fichiers et arborescences des serveurs et postes, avec une déduplication en blocs qui réduit très fortement le besoin de bande passante. Elle est idéale pour restaurer, **jusqu'au fichier unitaire**, des données effacées par erreur, corrompues ou chiffrées par un ransomware. Chez Cybee, c'est le mode universel, disponible sur Windows comme sur Linux.

Pour les bases de données et applications nécessitant une mise en cohérence dédiée, la bonne pratique consiste à sauvegarder les fichiers d'export (dumps) produits par l'application, qui sont ensuite dédupliqués et chiffrés comme les autres données. L'état de la prise en charge applicative est documenté dans la base de connaissances Cybee.

La sauvegarde en mode image de volume

La sauvegarde en mode image capture l'état complet d'un volume, ce qui simplifie la remise en service d'un serveur après un incident majeur : la restauration s'effectue au niveau du volume, en une seule opération, plutôt que fichier par fichier.

Chez Cybee, le mode image de volume est disponible pour les systèmes **Microsoft Windows** (en s'appuyant sur les mécanismes VSS du système). Les serveurs Linux sont sauvegardés en mode fichiers, ce qui correspond aux pratiques d'exploitation de ces environnements. Le mode de sauvegarde se choisit **par Plan de Sauvegarde**, dans la console d'administration.

La déduplication à la source : la bande passante maîtrisée

La consommation de bande passante est un facteur déterminant dans le choix d'une solution de sauvegarde en ligne. La réponse de Cybee est la **déduplication à la source** : avant transmission, l'agent découpe les données en fragments de taille variable dont l'empreinte cryptographique est comparée à celles déjà présentes dans le dépôt. Seuls les fragments nouveaux sont transmis et conservés.

Cette déduplication opère :

- **Entre sauvegardes successives** d'une même machine : chaque sauvegarde après la première ne transmet que les blocs modifiés, tout en produisant un cliché complet (chaque cliché est logiquement une sauvegarde totale, sans chaîne d'incréments fragile à reconstruire) ;
- **Entre machines partageant un même dépôt** : les fichiers systèmes ou applicatifs identiques présents sur plusieurs serveurs ne sont stockés qu'une seule fois.

Concrètement, les modifications quotidiennes représentent typiquement une faible fraction du volume total protégé. Ce mécanisme supprime au passage le dilemme classique « full hebdomadaire contre incrémentales quotidiennes » : avec un moteur dédupliqué, il n'est jamais nécessaire de retransmettre une sauvegarde complète, et il n'existe pas de chaîne d'incrémentales dont la corruption d'un maillon invaliderait la suite.

Full « perpétuelle » par conception : la plupart des solutions traditionnelles de sauvegarde doivent périodiquement exécuter des sauvegardes complètes (full), le modèle Cybee produit nativement, à chaque exécution, un cliché complet et intègre pour le « coût » réseau d'un incrément.

Un moteur open source : Restic, la transparence

Cybee s'appuie sur le moteur de sauvegarde open source **Restic**, utilisé dans sa version non modifiée et compilé par Cybee à partir des sources officielles (licence BSD 2-Clause). Ce choix d'architecture a des conséquences directes pour le client :

- **Transparence totale** : le code du moteur et le format cryptographique du dépôt sont publics, documentés et audités en continu par une large communauté internationale. Aucune boîte noire ;
- **Réversibilité réelle** : le format des dépôts est ouvert et publiquement documenté. En fin de contrat, les dépôts restitués au client sont exploitables avec les outils standard compatibles, sans aucune dépendance à l'égard de Cybee, sous réserve de la remise des clés de chiffrement, prévue contractuellement ;
- **Pérennité** : un moteur open source largement adopté ne disparaît pas avec son éditeur ; c'est une assurance de long terme pour des données dont la rétention peut se compter en années ;

- **Industrialisation par Cybee** : Cybee apporte au-dessus de ce moteur ce qui manque à l'open source brut pour l'entreprise : orchestrateur central, console d'administration multi-utilisateurs avec MFA, gestion des clés en coffre-fort, gestion des rôles et de la sécurité des utilisateurs, supervision, support et engagements de service (SLA).

Autour du moteur, la plateforme Cybee intègre d'autres composants open source éprouvés, comme ZITADEL (gestion des identités et authentification multifacteurs) et SpiceDB (gestion fine des autorisations par rôles).

L'immutabilité des sauvegardes

L'externalisation ne suffit plus : les attaquants recherchent et suppriment les sauvegardes distantes lorsqu'ils en obtiennent les accès. La réponse est l'**immutabilité du stockage objet (Object Lock)** : une fois écrite, une sauvegarde est verrouillée et ne peut être **ni modifiée, ni supprimée** pendant une durée de verrouillage paramétrable, y compris par un compte administrateur compromis.

Chez Cybee, l'immutabilité par Object Lock est également proposée sur l'Espace de Sauvegarde. Combinée au chiffrement à la source et à la rupture technologique du stockage objet, elle apporte la garantie centrale de la cyber-résilience : quoi qu'il arrive sur le site du client, il existe une copie intacte et restaurable.

À cette immutabilité s'ajoutent deux protections structurelles :

- **Redondance native** : les données sauvegardées sont répliquées sur deux ou trois zones de disponibilité (AZ Cloud), selon l'infrastructure d'hébergement retenue ;
- **Isolation** : chaque client dispose d'un conteneur de sauvegarde dédié, cloisonné des autres clients, et chaque dépôt de sauvegarde possède ses propres clés de chiffrement.

Le chiffrement de bout en bout

En fait vos données ne quittent jamais vos systèmes en clair. Le chiffrement est la base de la sécurité d'une sauvegarde en ligne. Deux approches existent sur le marché : soit le fournisseur chiffre les données côté serveur (et peut donc techniquement y accéder), soit les données sont chiffrées à la source, sur les systèmes du client, avant tout envoi. **Cybee applique strictement la seconde approche.**

Ce que fait techniquement Cybee

- **Chiffrement au repos** : toutes les données sont chiffrées par l'agent, à la source, en **AES-256 en mode authentifié** (schéma encrypt-then-MAC avec Poly1305-AES) : l'intégrité de chaque objet est vérifiée avant tout déchiffrement, et tout objet altéré est refusé ;
- **Chiffrement en transit** : les flux entre l'agent et l'Espace de Sauvegarde sont protégés par TLS (version minimale 1.2, TLS 1.3 privilégié), soit un double chiffrement, les données étant déjà chiffrées avant transport ;
- **Architecture de clés à deux niveaux** : chaque dépôt possède une **clé maître** unique, qui n'est jamais dérivée directement d'un mot de passe, et une ou plusieurs **clés d'accès**, dérivées chacune d'une phrase secrète distincte via une fonction de dérivation à coût mémoire élevé (scrypt), avec sel aléatoire ;

- **Rotation sans re-chiffrement** : le renouvellement d'une phrase secrète réencapsule la clé maître sans rechiffrer les données ; une clé d'accès peut être révoquée sans affecter les autres ;
- **Aucun accès en clair par Cybee** : les phrases secrètes sont conservées dans un coffre-fort technique dédié dont les mécanismes excluent tout accès des personnels de Cybee ; les clés sont injectées dans l'agent au moment de l'exécution et les opérations de chiffrement/déchiffrement s'exécutent exclusivement sur les systèmes du client.

Le meilleur des deux mondes. Le client bénéficie d'un chiffrement de bout en bout dont le fournisseur ne détient aucun accès en clair, sans supporter lui-même le risque de perte de clé : la garde des phrases secrètes est assurée par le coffre-fort de Cybee, et les clés sont restituées au client dans le cadre de la réversibilité contractuelle.

La résistance post-quantique contre les menaces de demain

La cryptographie post-quantique fait référence aux dispositifs conçus pour maintenir leur sécurité face à l'avènement des ordinateurs quantiques. Dans le domaine de la sauvegarde, l'enjeu est important : on parle de la menace de « collecter maintenant, déchiffrer plus tard ». Un attaquant qui récupère aujourd'hui des sauvegardes cryptées, ayant une durée de rétention pouvant s'étaler sur plusieurs années, pourrait essayer de les déchiffrer dès que l'informatique quantique sera disponible.

L'informatique quantique (via l'algorithme de Shor) représente une menace pour certains algorithmes, plus particulièrement ceux **asymétriques** tels que RSA et les courbes elliptiques. Quant à la cryptographie **symétrique**, elle ne fait que subir une accélération de l'algorithme de Grover, qui réduit la sécurité effective de moitié : Un chiffrement AES-256 maintient une robustesse comparable à celle d'un 128 bits, considéré comme sûr même face à un ordinateur quantique.

L'architecture cryptographique du dépôt Cybee se base exclusivement sur des mécanismes symétriques (scrypt pour la dérivation de clés, AES-256 pour le chiffrement, Poly1305-AES pour l'authentification, SHA-256 pour l'adressage des objets) : aucune clé asymétrique n'intervient dans la protection des données stockées. Les informations contenues dans un dépôt Cybee sont ainsi protégées contre les attaques quantiques identifiées.

Sur le marché, la majorité des discussions « **post-quantiques** » se concentrent sur des feuilles de route.

La résistance quantique des sauvegardes Cybee ne dépend pas d'évolutions futures : elle découle du choix, dès l'origine, d'un format de dépôt entièrement symétrique, et d'autres solutions de sécurité publiques et documentées.

Restauration : la seule métrique qui compte le jour J

Une sauvegarde non testée est une sauvegarde présumée défaillante

Tant que la restauration n'est pas testée régulièrement, vous prenez le risque d'une très mauvaise surprise le jour où vous en avez besoin. Pour reprendre l'image du chat de Schrödinger : une sauvegarde est à la fois valide et invalide, et c'est seulement à la restauration que son état réel se révèle.

Les études du secteur donnent la mesure du problème : **46 %** des organisations n'ont jamais effectué de test de restauration de leurs systèmes de sauvegarde [1], et lorsque les tests ont lieu, **42 %** des tentatives aboutissent à des données inaccessibles ou inexploitables [2]. Les organisations qui testent moins d'une fois par an présentent des taux d'échec nettement plus élevés [3].

Cybee facilite cette discipline à deux niveaux :

- **Vérifications d'intégrité des dépôts** : une vérification rapide est réalisée après chaque sauvegarde, et des vérifications approfondies sont conduites à intervalles réguliers, le tout sur les données chiffrées, sans jamais accéder à leur contenu. Le client peut en outre déclencher ou programmer ses propres vérifications depuis la console ;

- **Restauration en autonomie** : le client restaure lui-même, à tout moment, depuis la console et l'agent, jusqu'au fichier unitaire en mode fichiers, au niveau du volume en mode image vers l'emplacement d'origine, un autre emplacement, ou une autre machine équipée de l'agent. Tester une restauration ne nécessite ni ticket, ni intervention de l'éditeur.

Performance de restauration

En cas de sinistre majeur, le facteur limitant est le débit de restauration. L'architecture Cloud-first de Cybee (stockage objet, parallélisation des flux) permet des débits de restauration dans le Cloud jusqu'à **3 To/h**, de quoi remettre en service des volumétries significatives en heures et non en jours.

Le chargement initial des données dans le Cloud

Le temps du premier chargement complet est corrélé au débit ascendant de la liaison Internet. Lorsque le volume de données ou le débit disponible ne permettent pas un chargement initial par le réseau dans des délais raisonnables, Cybee propose une **Option Chargement Initial** : un serveur de stockage amovible est mis à disposition pour réaliser la première sauvegarde complète localement.

Point de sécurité essentiel : les données transférées sur ce support sont chiffrées à la source par l'agent, dans les mêmes conditions que les sauvegardes réseau ; elles ne quittent jamais les systèmes du client en clair. Le support est ensuite acheminé et les clichés sont intégrés à l'Espace de Sauvegarde ; les sauvegardes suivantes, dédupliquées, ne transmettent plus que les blocs modifiés.

Hébergement européen, droit européen, zéro transfert hors UE

Pour des sauvegardes, qui contiennent par nature l'intégralité du patrimoine informationnel de l'entreprise, la localisation des données et le droit applicable ne sont pas des détails.

Les engagements Cybee

- **Hébergement exclusivement dans l'Union européenne** : les Espaces de Sauvegarde sont hébergés, sous forme de stockage objet dans de Clouds de droit européen ;
- **Aucun transfert hors UE/EEE** : aucun sous-traitant ultérieur de Cybee n'est établi hors de l'Union européenne ou de l'Espace économique européen, et aucun traitement réalisé au titre du service n'implique de transfert de données personnelles hors UE/EEE ;
- **Infrastructures certifiées** : datacenters certifiés ISO/IEC 27001 et HDS (Hébergeur de Données de Santé);
- **Transparence contractuelle** : les hébergeurs sont nommés dans les documents contractuels ; tout changement est soumis à préavis, au maintien de la localisation UE et à un niveau de certification au moins équivalent.

Cloud Act, extraterritorialité : le droit compte autant que la géographie

Depuis l'invalidation du Privacy Shield par la Cour de justice de l'Union européenne (arrêt « Schrems II », 2020 et l'arrivé d'un potentiel « Schrems III » en 2026), les transferts de données vers les États-Unis reposent sur des cadres juridiques régulièrement contestés. Surtout, le **Cloud Act** américain permet aux autorités des États-Unis, dans le cadre d'une procédure judiciaire, d'exiger d'un fournisseur soumis au droit américain l'accès à des données **où qu'elles soient stockées**, y compris dans un datacenter situé en Europe.

Choisir un éditeur basé en Europe, hébergé chez des opérateurs de droit européen, offrant un chiffrement de bout en bout auquel l'éditeur n'a pas accès en clair, permet d'éviter ce conflit de lois dès le départ. Il est aussi important de prêter attention aux transferts de données : certaines propositions conservent les données en Europe, mais assurent le passage des flux, de la télémétrie ou des métadonnées par des infrastructures qui ne sont pas situées en Europe.

RGPD et NIS 2 : la sauvegarde devient une obligation réglementaire

Le RGPD impose de garantir la sécurité des données personnelles, leur disponibilité et leur capacité de rétablissement après incident (article 32). La directive **NIS 2**, en cours de transposition en droit français sous l'égide de l'ANSSI, va plus loin : elle impose explicitement aux entités essentielles et importantes des mesures de gestion des risques incluant **la continuité d'activité, la gestion des sauvegardes et la reprise après sinistre**. Une sauvegarde externalisée, immuable, chiffrée et testée n'est plus seulement une bonne pratique : elle devient un élément de conformité.

L'orchestrateur Cybee : l'industrialisation de la sauvegarde

La différence entre un outil de sauvegarde et un service de sauvegarde d'entreprise se joue dans l'orchestration. L'Orchestrateur Cybee est le service central qui coordonne automatiquement l'ensemble des opérations :

- **Planification** : chaque Plan de Sauvegarde est lié à une ou plusieurs planifications (syntaxe calendaire standard, fuseau horaire explicite), sans planification imposée par défaut : les fenêtres de sauvegarde sont ajustées en fonction des contraintes opérationnelles du client ;
- **Rétention et élagage** : les clichés expirés sont automatiquement supprimés à l'échéance de la Période de Rétention, puis les données non référencées sont supprimées lors d'un processus de nettoyage séparé, également programmé ;
- **Gestion des priorités et des accès simultanés :** l'orchestrateur hiérarchise les opérations, contrôle les priorités et empêche l'usage simultané d'une même ressource, pour garantir que les tâches soient réalisées dans l'ordre et au moment prévu ;
- **Flexibilité des dépôts** : un Plan de Sauvegarde peut couvrir un serveur unique ou un groupe de machines mutualisées sur un même dépôt (maximisant la déduplication inter-machines) ; des rétentions distinctes s'obtiennent par des plans dédiés.

La Console Cybee : piloter et superviser en toute autonomie

La Console Cybee (app.cybee.fr) est l'interface d'administration en ligne du service. Elle permet notamment:

- De gérer les utilisateurs et administrateurs, avec un modèle de droits fondé sur les rôles et une authentification multifacteurs (MFA) obligatoire ;
- De créer et modifier les Plans de Sauvegarde, leurs planifications et leurs rétentions ;
- De suivre la consommation de l'Espace de Sauvegarde (le dépassement de capacité n'est jamais bloqué techniquement : il déclenche alertes et notification) ;
- De consulter les rapports d'exécution, de recevoir des alertes automatiques par e-mail et de vérifier l'état et l'intégrité des dépôts, manuellement ou de manière programmée.

Le service Cybee est un service **non managé** : le client conserve la maîtrise et la supervision de ses sauvegardes, avec tous les outils pour l'exercer, et bénéficie d'un support (e-mail et téléphone) comme aide à l'utilisation. Ce modèle, transparent, se distingue des offres managées, comme celles opérées par des partenaires de Cybee, qui prennent en charge la supervision pour le compte du client.

Engagements de service (SLA)

- Disponibilité de l'Espace de Sauvegarde (écriture des sauvegardes et lecture pour restauration) : taux cible de **99,9 % par mois civil**, assorti de crédits de service en cas de non-atteinte ;
- Disponibilité de la Console : taux cible de **99,5 % par mois civil** ;
- Garanties de temps d'intervention du support selon le niveau de priorité, en heures ouvrées.

Trois scénarios d'utilisation typiques

Scénario 1 : PME avec serveurs virtuels, sauvegarde internalisée

L'entreprise dispose d'une dizaine de serveurs importants, sauvegardés sur médias chaque semaine dans un coffre. L'informaticien vérifie chaque jour les sauvegardes, sans jamais avoir le temps de tester une restauration.

L'apport de Cybee : externalisation automatique et chiffrée vers un dépôt immuable, alertes automatiques par e-mail, vérification d'intégrité après chaque sauvegarde, et tests de restauration réalisables à tout moment, sans manipulation physique de supports.

Scénario 2 : ETI avec parc hétérogène Windows et Linux on-premise et Cloud

L'entreprise exploite un mix de serveurs on-premise et dans un Cloud public, Windows et Linux, avec aujourd'hui deux solutions de sauvegarde distinctes à superviser (locale et Cloud).

L'apport de Cybee : un agent unique multi-plateforme (Windows et Linux, physique, virtuel, quel que soit l'hyperviseur, et Cloud), un mode image de volume pour Windows et un mode fichiers universel, le tout piloté depuis une console unique. Un seul outil, une seule supervision, un seul dépôt dédupliqué.

Scénario 3 : postes de travail et collaborateurs mobiles

Les collaborateurs en déplacement stockent sur leur portable des données clients, sauvegardées, au mieux, sur un média externe, avec les risques d'oubli, de perte et de vol associés.

L'apport de Cybee : l'agent s'installe aussi sur les postes de travail fixes et portables ; les données sont sauvegardées automatiquement, chiffrées à la source, dès qu'une connexion réseau est disponible, et restaurables sur une autre machine du même client équipée de l'agent.

Les bénéfices de la sauvegarde Cloud cyber-résiliente

- **Résister aux ransomwares** : étanchéité par rupture technologique, immutabilité Object Lock, chiffrement de bout en bout ;
- **Réduire les coûts** : déduplication à la source, stockage objet économique, suppression des investissements matériels et des manipulations de supports (CAPEX → OPEX) ;
- **Libérer les équipes** : orchestration automatique des sauvegardes, de la rétention et de l'élagage ; alertes plutôt que vérifications manuelles quotidiennes ;
- **Prouver la conformité** : hébergement 100 % UE, RGPD natif, alignement sur les exigences NIS 2 en matière de sauvegarde et de continuité ;
- **Garder la maîtrise** : format ouvert, réversibilité contractuelle avec restitution des dépôts et des clés, zéro dépendance éditeur.

Questions fréquentes

Pourquoi choisir une solution de sauvegarde basée sur Restic ?

Restic est un moteur de sauvegarde open source (licence BSD 2-Clause) dont le format de dépôt est public, documenté et audité par une large communauté. Il apporte nativement la déduplication à la source, le chiffrement AES-256 authentifié et des clichés complets à chaque exécution. Cybee l'utilise dans sa version non modifiée et l'industrialise pour l'entreprise : orchestrateur, console avec MFA, gestion des clés, supervision, SLA et support.

Est-ce que Cybee est capable de consulter le contenu de mes backups ?

Non. Les données sont chiffrées dès le point d'origine, sur vos systèmes, avant toute transmission, et les processus de déchiffrement sont strictement réalisés sur ces mêmes systèmes. Les mots de passe sont stockés dans un coffre-fort numérique dont le fonctionnement empêche tout accès en clair par les employés de Cybee.

Où sont hébergées les données sauvegardées ?

Uniquement au sein de l'Union européenne : sur T Cloud Public (T-Systems, groupe Deutsche Telekom en Allemagne et Pays-Bas) ou chez Leviia (France, à Lyon ou Marseille, certifié ISO/IEC 27001 et HDS). Le service n'implique aucun transfert de données personnelles en dehors de l'UE/EEE.

Que se passe-t-il si je quitte Cybee ?

La réversibilité est contractuelle : Cybee restitue l'intégralité de vos dépôts, la configuration associée et les clés de chiffrement nécessaires, sur un espace S3 sécurisé. Le format des dépôts étant ouvert, ils restent exploitables avec les outils standard compatibles, sans dépendance à l'égard de Cybee.

Qu'est-ce qu'une sauvegarde immuable ?

Une sauvegarde immuable est une sauvegarde qui, une fois écrite, ne peut être ni modifiée ni supprimée pendant une durée de verrouillage définie, grâce au mécanisme Object Lock du stockage objet S3. Même un attaquant disposant d'identifiants d'administration valides ne peut pas la détruire. C'est la protection de référence contre les ransomwares qui ciblent les sauvegardes.

Les sauvegardes Cybee résistent-elles aux ordinateurs quantiques ?

La protection des données au repos repose exclusivement sur des primitives symétriques (AES-256, Poly1305-AES, scrypt, SHA-256), qui ne sont pas menacées par l'algorithme de Shor. AES-256 conserve, face à l'algorithme de Grover, une sécurité effective de 128 bits, considérée comme sûre y compris dans un contexte quantique.

Conclusion

La sauvegarde en ligne a atteint une maturité, fonctionnalités, performances, sécurité, qui permet aux PME, ETI et organismes publics de disposer de solutions à la fois plus sûres et moins coûteuses que les architectures traditionnelles. Mais toutes les sauvegardes Cloud ne se valent pas face aux ransomwares.

La cyber-résilience exige un ensemble cohérent : rupture technologique par le stockage objet, immutabilité, chiffrement de bout en bout sans accès de l'éditeur, déduplication à la source, vérifications d'intégrité systématiques et restaurations testables à volonté. Elle exige aussi, pour des données qui constituent le patrimoine complet de l'entreprise, des garanties de souveraineté : hébergement européen, droit européen, format ouvert et réversibilité.

C'est l'ensemble de ces exigences que Cybee a réunies dans une solution unique, construite sur un moteur open source éprouvé et industrialisée pour l'entreprise et, par la conception entièrement symétrique de sa cryptographie, déjà prête pour l'ère post-quantique.

Vous avez un projet de sauvegarde cyber-résiliente de vos serveurs ?

Les équipes Cybee vous accompagnent pour étudier la faisabilité dans votre contexte (volumétrie, bande passante, modes de sauvegarde), dimensionner votre Espace de Sauvegarde et définir vos Plans de Sauvegarde.

Cybee : Demandez une démonstration

Support et contact : support@cybee.fr | +33 (0)4 28 29 79 01

Sources

[1] **Unitrends, State of Backup and Recovery Report 2025** : 46 % des organisations n'ont jamais effectué de test de restauration de leurs systèmes de sauvegarde ; 23 % des entreprises ne testent jamais leurs sauvegardes. Données relayées par SnapshotShield : *snapshotshield.com/backup-testing-research.html*.

[2] **Veeam, Data Protection Trends Report 2024** : 58 % des serveurs testés ont pu être restaurés dans les délais prévus par les SLA ; dans 42 % des cas, les données étaient inaccessibles ou inexploitables ; 13 % des entreprises disposent d'une orchestration automatisée de leur plan de reprise d'activité. Données relayées par Sigilence Technologies : *blog.sigilence-technologies.com/fr/blog/2025/10/20/data-backup-and-recovery/*.

[3] **TWC IT Solutions / Invenio IT** (synthèses de plusieurs études) : 50 % des entreprises testent leur plan de reprise d'activité au moins une fois par an ; les organisations qui testent moins d'une fois par an présentent des taux d'échec nettement plus élevés. Données relayées par SnapshotShield : *snapshotshield.com/backup-testing-research.html*.

Les définitions de « test régulier » variant selon les études (test annuel, test avant changement majeur, test de restauration unitaire vs test de PRA complet), les chiffres ci-dessus sont donnés à titre d'ordre de grandeur. Les rapports d'origine (Unitrends, Veeam) constituent les sources primaires de référence.