POURQUOI LA PROTECTION, LA SÉCURITÉ, ET L'IA DOIVENT CONVERGER

COHESITY

POURQUOI LA PROTECTION, LA SÉCURITÉ, ET L'IA DOIVENT CONVERGER

Depuis des années, les entreprises ont abordé la protection des données, la sécurité des données et les projets d'IA comme des chantiers séparés. Les équipes de sauvegarde, quant à elles, étaient principalement mobilisées sur la capacité de récupération, de restauration et de reprise. Les équipes de sécurité privilégiaient la prévention des menaces. Les équipes en charge de l'IA se focalisaient sur l'analyse, l'automatisation et l'innovation. Chaque équipe opérait avec ses propres outils, objectifs et architectures.

Il est temps de repenser ce modèle fragmenté.

Les raisons en sont concrètes : les cyberattaques sont de plus en plus ciblées, et les données résident désormais partout, en local, dans le cloud et dans l'ensemble des environnements SaaS. Parallèlement, les entreprises éprouvent des difficultés à accéder aux données afin d'améliorer leurs performances et résultats de leurs projets liés à l'IA. Or ces données sont fréquemment fragmentées entre des systèmes disparates, augmentant la complexité et les zones d'ombre.

Multiplier les outils ne permet pas de résoudre ce problème. Cela tend au contraireà l'accentuer.

Les entreprises qui se démarquent ne reposent pas sur une superposition de couches d'outils supplémentaires.

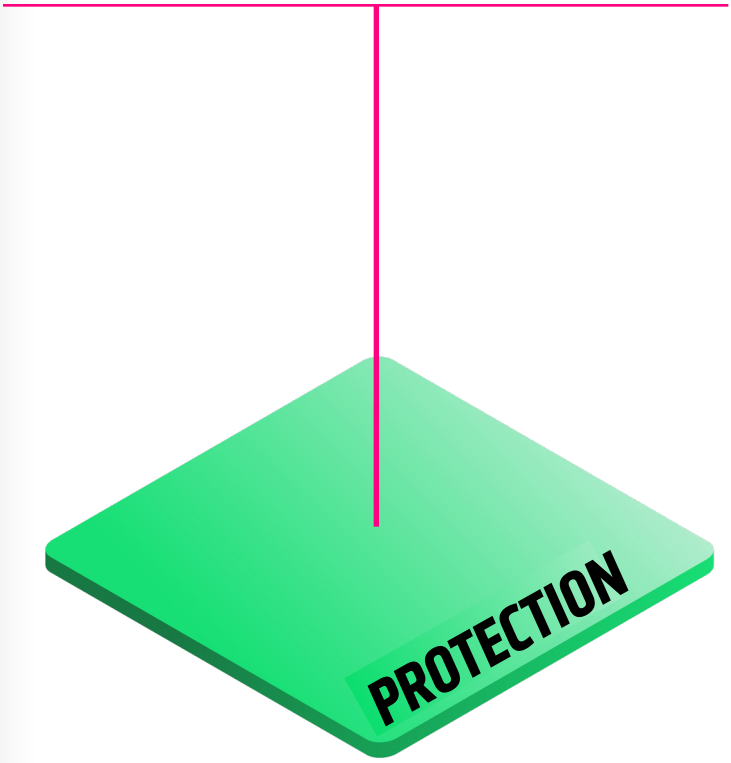
Les acteurs les plus avancés en repensent les bases.

PROTECTION
la protection.

La protection constitue la première étape de la cyber-résilience. Tout commence par une couverture complète de l'ensemble de votre patrimoine de données, des machines virtuelles aux bases de données, en passant par les systèmes de fichiers et les charges de travail non structurées.

La protection doit s'appliquer à l'ensemble de ces données, de façon homogène et sans angle mort. La restauration et la reprise des activités en dépendent. Lorsque la protection est incomplète, fragmentée ou incohérente, il devient impossible de garantir une restauration rapide et saine. En revanche, lorsqu'elle est exhaustive et cohérente, cela devient possible, sans corruption, sans perte ni risque résiduel.

La cyber-résilience commence par ce niveau fondamental de protection.



LA SÉCURITÉ doit être intégrée à la couche de données

Une fois la protection en place, le défi suivant apparaît clairement :

si les systèmes de sauvegarde peuvent être compromis, chiffrés ou consultés de manière inappropriée, les données de restauration elles-mêmes deviennent une nouvelle surface d'attaque. La sécurité ne peut plus être traitée comme une surcouche externe. Elle doit s'exercer directement au niveau de la couche où résident les données.

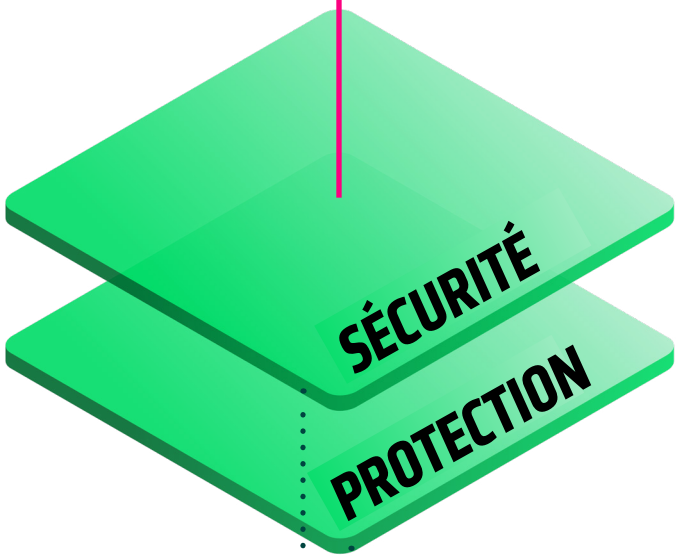
Cela signifie :

- Détecter les activités anormales au sein des environnements de sauvegarde
- L'application de contrôles de l'identité et des accès à la source
- La mise en œuvre d'une gouvernance cohérente à l'échelle de l'ensemble du patrimoine de données

Lorsque protection et sécurité s'appuient sur des systèmes distincts, les équipes doivent corréler les alertes/indicateurs et harmoniser les politiques entre les différents outils, souvent dans un contexte d'urgence et de forte contrainte opérationnelle. Les lacunes n'apparaissent pas faute de capacités, mais parce que celles-ci ne sont pas intégrées au sein d'un ensemble cohérent.

L'intégration de la sécurité à la couche de protection des données comble ces lacunes et permet aux mesures de sécurité et de restauration de se renforcer réciproquement. La détection des menaces contribue à l'intégrité de la restauration et la gouvernance est définie une seule fois, puis mise en œuvre et contrôlée à l'échelle de l'ensemble des environnements.

Ensemble, elles posent les bases d'un environnement de données de confiance.



La protection pose les bases
de la résilience.

Sécurité
la renforce.

L'IA peut alors être mise en œuvre de manière concrète à l'échelle de l'entreprise

Ce n'est qu'après avoir assuré une protection et une sécurisation fiables des données que de nouvelles possibilités se révèlent pleinement.

Pour que l'IA produise des résultats concrets, les entreprises doivent :

- Centraliser les données non structurées sur l'ensemble des environnements
- Conserver l'historique des évolutions et des modifications
- Maintenir une gouvernance cohérente, un contrôle d'accès basé sur les rôles et une auditabilité de bout en bout
- Réduire les risques de duplication et d'exposition involontaire

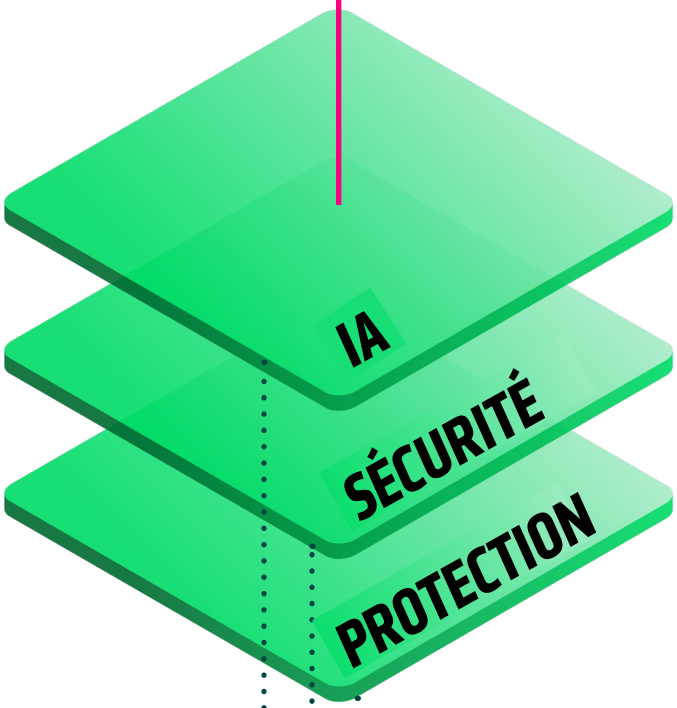
De nombreuses équipes cherchent à répondre à cet enjeu en répliquant les données dans des plateformes d'analyse ou d'IA distinctes. Il en résulte des coûts plus élevés, une complexité renforcée et une surface d'attaque élargie.

Une base unifiée change cette dynamique. Elle permet aux entreprises d'accéder à des données adaptées à l'IA et de les exploiter en toute sécurité, avec exactitude et sans lacunes.

Lorsque la protection et la sécurité sont déjà intégrées, ce même environnement de données de confiance peut être rendu détectable et exploitable, sans altérer les modèles de gouvernance ni dupliquer les données et l'infrastructure. Les données qui assurent la continuité deviennent alors des données adaptées à l'IA, au service de l'analyse et de la production de renseignements.

Dans ce modèle, l'IA joue deux rôles. Elle améliore la plateforme sous-jacente grâce à l'automatisation et à une détection plus intelligente. Elle alimente aussi tout un éventail d'applications, des assistants de productivité aux agents spécialisés, en s'appuyant sur des données d'entreprise gouvernées comme socle de référence.

Chaque couche s'appuie sur celle qui la précède.



La protection rend les données récupérables.

La sécurité garantit leur intégrité.

L'IA en fait un levier de valeur.

CETTE CONVERGENCE s'impose.

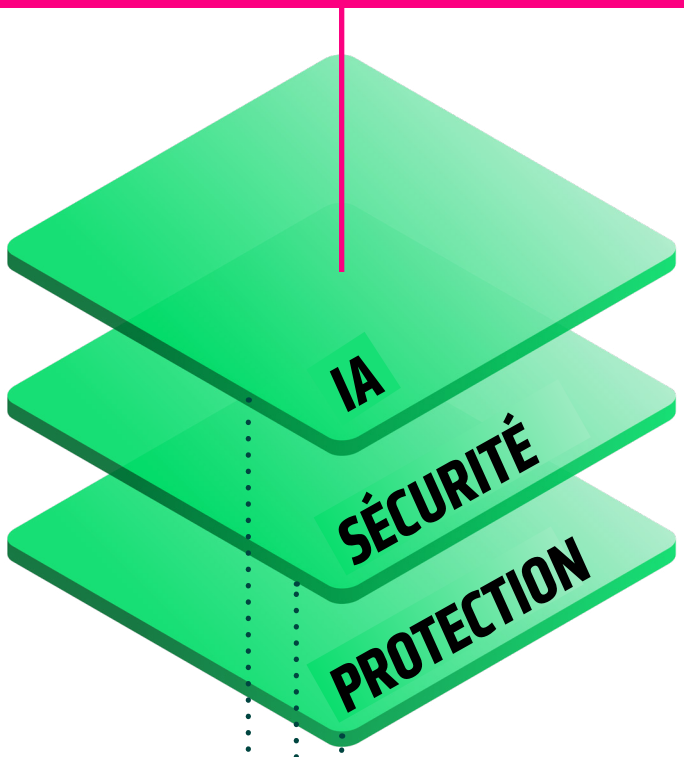
Lorsque protection, sécurité et préparation à l'IA reposent sur un socle commun, vos données sont :

- Soumises à une gouvernance unique et exploitables pour de multiples usages
- Protégées quel que soit leur emplacement
- Sécurisées à la source
- Rendues adaptées à l'IA, sans duplication

Soudain, la copie la plus sûre de vos données devient aussi la plus intelligente.

Dans un monde façonné par le cyber-risque et l'accélération de l'adoption de l'IA, le choix d'architecture ne fait plus de doute : un patrimoine de données unifié, administré comme un système unique et évolutif, conçu pour résister aux perturbations tout en produisant des connaissances exploitables.

C'EST L'AMBITION DE COHESITY DATA CLOUD.



La protection assure la capacité de récupération.

La sécurité réduit l'exposition au risque.

L'IA en révèle la valeur.

UNE APPROCHE ÉPROUVÉE À L'ÉCHELLE DE L'ENTREPRISE.

Cohesity Data Cloud est la seule plateforme unifiée conçue pour renforcer votre cyber-résilience et révéler tout le potentiel de vos données.

Elle protège **plus de 1 000** charges de travail en local, dans le cloud et dans les environnements SaaS, avec des sauvegardes jusqu'à **18 fois** plus rapides, des restaurations **97 %** plus rapides, et une amélioration de la rentabilité de l'IA quasi immédiate, le tout avec **50 %** de stockage en moins et jusqu'à **40 %** d'économies sur le coût total.

En savoir plus sur cohesity.com/DataCloud

COHESITY
cohesity.com/fr/
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

6300010-001-FR 03-2026