

Etude du marché PRA & DraaS en France

Solutions de PRA / Disaster Recovery
Plan dans les environnements cloud
auprès de la clientèle mid market



Avant-propos

Les solutions de Plan de Reprise d'Activité (PRA) visent à assurer la continuité ou la reprise d'activité rapide organisations. Le PRA permet de :

- Maintenir les opérations malgré un sinistre,
- Sécuriser la poursuite d'activité de l'entreprise, de l'organisation,
- Réduire les éventuelles conséquences financières d'un arrêt de service.

Avec le développement des infrastructures cloud, l'association de cloud avec des infrastructures de type cloud privé, legacy ou sur site et non virtualisées dans des environnements hybrides et multicloud oblige à repenser les schémas de protection des données. En parallèle, l'explosion du nombre de cybermenaces avec leurs conséquences désastreuses sur l'activité des entreprises accentue le mouvement vers de nouveaux PRA. Enfin, les réglementations poussent les obligés à se conformer et instaurer des nouvelles solutions.

Bien que la plupart des ETI et grandes organisations, disposent déjà de solutions de protection des données pour la sauvegarde et la reprise d'activité, de nouveaux enjeux et de nouvelles innovations poussent les

entreprises à moderniser leurs PRA. L'étude présente réalisée pour le compte d'Orange Business met en lumière la dimension du marché et ses perspectives d'évolution, ses acteurs tant prestataires de services qu'éditeurs de solutions logicielles, les principales tendances du marché et les défis actuels. Parmi les défis, le développement des architectures SaaS et cloud-native qui demandent plus d'évolutivité et de mobilité des données que des applications traditionnelles et legacy. Les solutions de PRA et protection des données s'adaptent, évoluent et vont désormais au-delà des simples logiciels sur site et des appliances pour inclure des services de sauvegarde en ligne et de reprise Disaster Recovery as a Service (DRaaS).

Contre les multiples menaces, les entreprises souhaitent aujourd'hui mieux protéger et restaurer leurs applications et données critiques. L'évolution du marché des solutions de PRA suit ces tendances avec des acteurs qui proposent désormais des couvertures techniques élargies, des capacités de récupération après cyberattaque et des modèles d'utilisation plus performants et plus interopérables (SaaS). La protection des données et la reprise d'activité forment désormais un élément essentiel de l'infrastructure informatique.

Sommaire

- 01** Le marché du PRA et DRaaS en France
- 02** Les enjeux de sauvegarde et continuité d'activité
- 03** Les solutions de sauvegarde et PRA

01

Le marché du PRA et DRaaS en France

Contexte, données de marché et perspectives d'évolutions

Périmètre du PRA et DRaaS dans la data-résilience

Data-résilience				
Gouvernance et stratégie de résilience	Infrastructures de résilience (IT & Cloud)	Détection et réponse aux incidents	Résilience des utilisateurs et de la culture cyber	Assurance et financement de la résilience
Objectif : Anticiper, piloter et coordonner les dispositifs de résilience. - Gouvernance des risques IT / cyber - Plan de Continuité d'Activité (PCA) & Plan de Reprise d'Activité (PRA) - Audit de résilience et de maturité - Conformité réglementaire - Résilience organisationnelle	Objectif : Garantir la reprise technique rapide des services en cas d'incident - PRA / PCA managés (on-premise, cloud privé, cloud public souverain) - Backup et restauration - Solutions de réplication et haute disponibilité - Continuité applicative (BIA, orchestration PRA) - Jumeaux numériques et simulation de crise Périmètre d'analyse	Objectif : Réduire l'impact opérationnel des cyberattaques. - SOC managés / CSIRT / CERT - Services de réponse à incident (forensic, remédiation) - Cyber Threat Intelligence (CTI) - Plans de gestion de crise cyber - Simulations de crise, exercices de résilience	Objectif : Renforcer le facteur humain, limiter les vecteurs d'attaque internes. - Formation et sensibilisation à la cyberrésilience - Tests de phishing & campagnes de sensibilisation - Plans de communication de crise - Assistance psychologique post-attaque (rare mais en croissance)	Objectif : Cadrer financièrement les risques et les coûts liés aux interruptions. - Cyber-assurance avec volet PCA/PRA - Évaluation financière de la résilience / scoring - Solutions de transfert ou mutualisation du risque

Contexte

Le marché de la data-résilience en France

Data-résilience	2023	2024	2025	2026	2027	2028
PRA and DRaaS	598	629	663	699	733	766
Managed Services (SOC, CERT/CSIRT ...)	429	499	584	682	791	918
Conseil et Audit cyber résilience	274	295	312	330	351	373
Formation	225	241	259	277	296	316
Total Marché	1526	1665	1818	1988	2171	2373

Data-résilience	23/24	24/25	25/26	26/27	27/28	CAGR 24/28
PRA and DRaaS	5,2%	5,4%	5,4%	4,9%	4,5%	5,0%
Managed Services (SOC, CERT/CSIRT ...)	16,2%	17,0%	16,7%	16,0%	16,0%	16,4%
Conseil et Audit cyber résilience	7,7%	5,7%	5,9%	6,4%	6,3%	6,1%
Formation	7,4%	7,3%	7,1%	6,8%	6,8%	7,0%
Total Marché	9,1%	9,2%	9,4%	9,2%	9,3%	9,3%

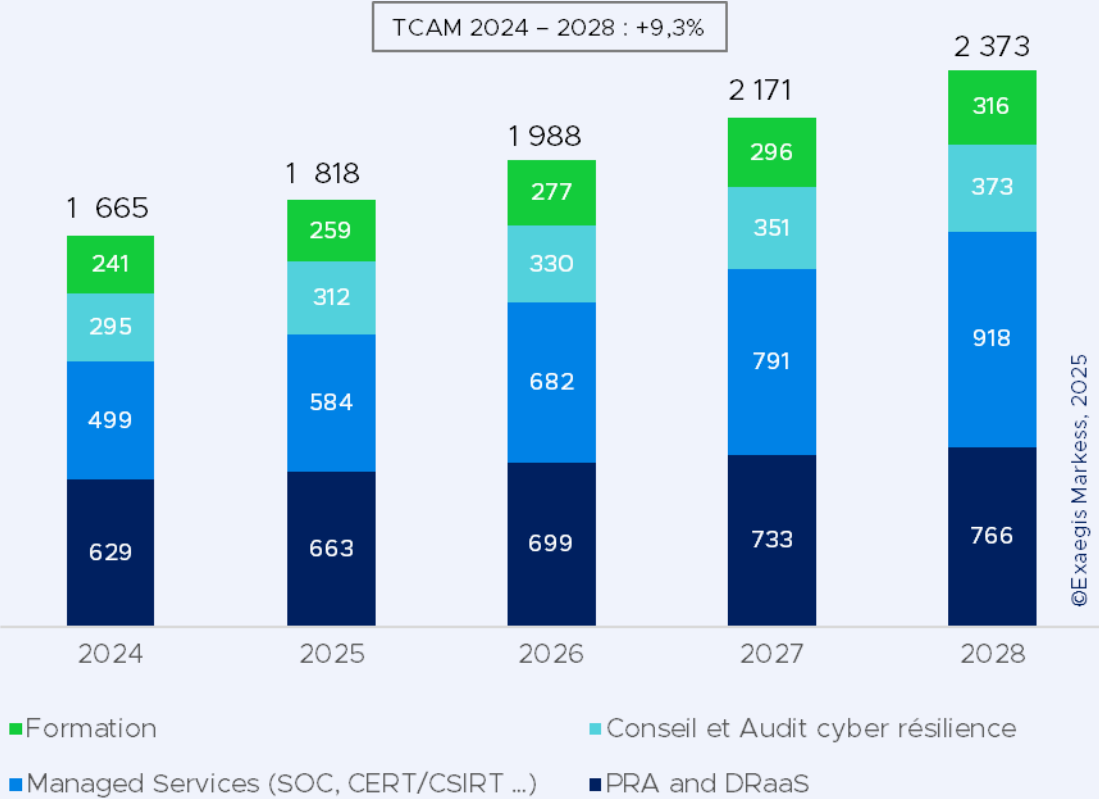
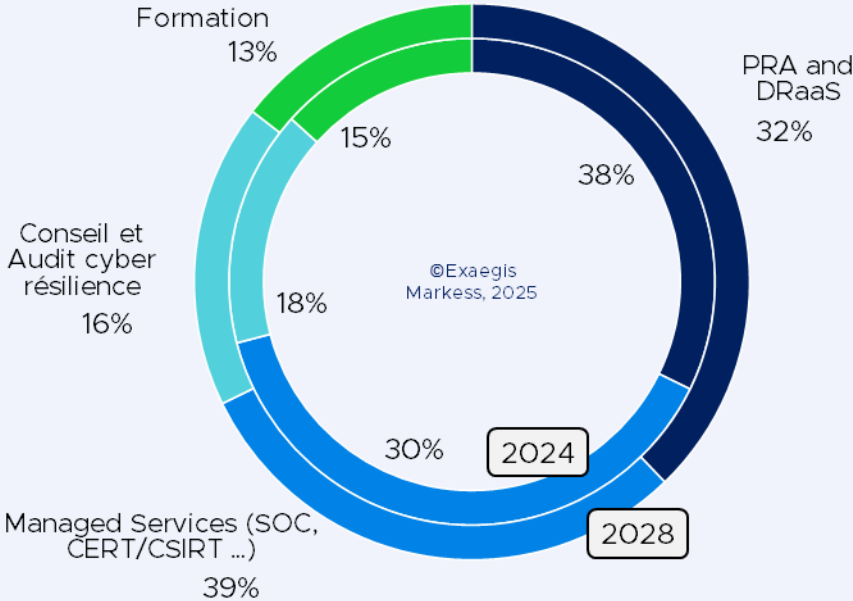
Le marché total lié à la data-résilience en France était de 1,7 milliards d’euros en 2024. Sa croissance devrait être tirée par les prestations de managed services en cybersécurité.

Facteurs clés de croissance du marché de la cyber-résilience

- Hausse du risque cyber : Intensification des attaques (ransomware, supply chain, etc.) => besoin accru de continuité d’activité.
- Pression réglementaire et normative : Renforcement des obligations réglementaires (RGPD, NIS2, DORA LPM) et des référentiels (ISO 27001, SecNumCloud, PDIS) => conformité, traçabilité et plans de reprise obligatoires.
- Transformation IT : Adoption massive du cloud et des architectures hybrides => nécessité d’une résilience adaptée aux nouveaux environnements.
- Extension du marché cible : Après les grands comptes et les ETI, accélération de la demande côté PME, encouragée par les assureurs, les MSSP et les initiatives publiques (France Relance, cyberscore, etc.).

Contexte

Le marché de la data-résilience en France



Le marché du PRA et DRaaS en France

PRA & DRaaS	2023	2024	2025	2026	2027	2028
Logiciels & Appliances on premise	289	292	294	294	289	282
Logiciels SaaS	81	92	106	121	138	155
Total logiciels & Appliances	370	384	400	415	427	437
Professional Services	132	140	148	156	162	168
Managed Services	96	105	115	128	144	161
Total Services	228	245	263	284	306	329
Total Marché	598	629	663	699	733	766

PRA & DRaaS	24/23	25/24	26/25	27/26	28/27	CAGR 28/24
Logiciels & Appliances on premise	1,0%	0,7%	0,0%	-1,7%	-2,4%	-0,9%
Logiciels SaaS	13,6%	15,2%	14,2%	14,0%	12,3%	13,9%
Total logiciels & Appliances	3,8%	4,2%	3,8%	2,9%	2,3%	3,3%
Professional Services	6,1%	5,7%	5,4%	3,8%	3,7%	4,7%
Managed Services	9,4%	9,5%	11,3%	12,5%	11,8%	11,3%
Total Services	7,5%	7,3%	8,0%	7,7%	7,5%	7,6%
Total Marché	5,2%	5,4%	5,4%	4,9%	4,5%	5,0%

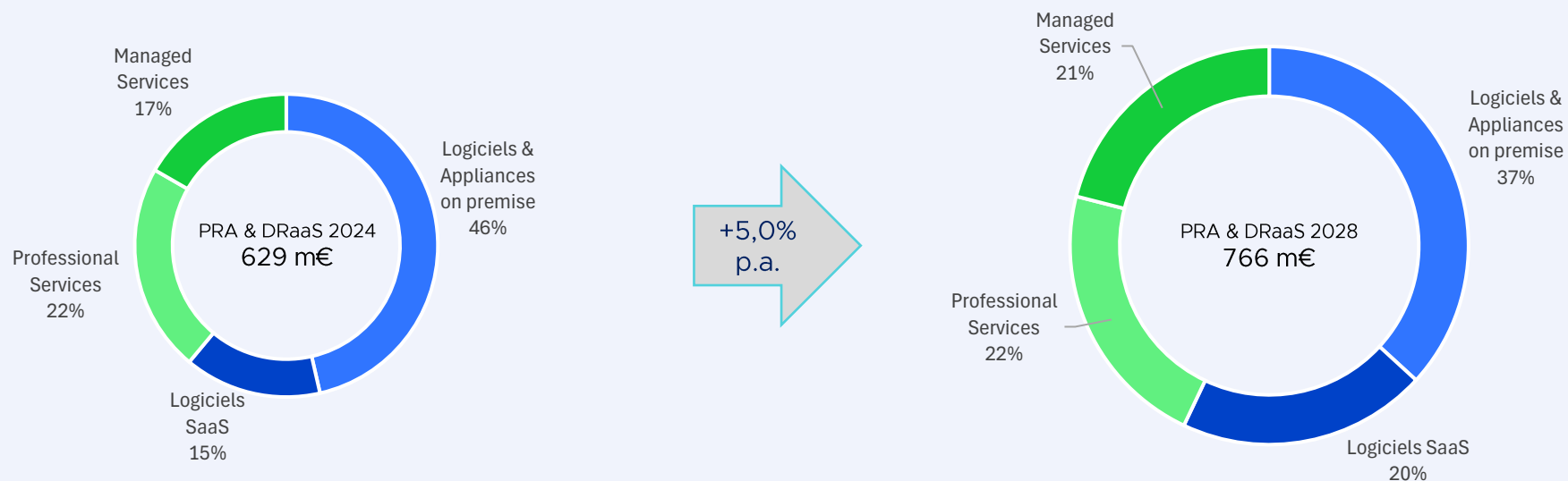
Le développement rapide des cyber menaces et les réglementations DORA, NIS2 et le Cyber Resilience Act poussent les organisations à mettre en œuvre des solutions de maintien et de reprise d'activité solides. Cela tire le marché total des logiciels et appliances dédiés au PRA et au DRaaS qui était de 384 m€ en 2024, majoritairement composé de solutions on-premise.

D'ici 2028, la dynamique du SaaS sera très forte (+14% de moyenne), mais ne permettra pas à ce segment de devenir majoritaire.

Le développement des solutions SaaS associé à l'engouement pour le multicloud et le cloud hybride favoriseront le développement des managed services, prestations nécessaires pour mieux gérer la complexité des environnements multiples.

Les sous-jacents du marché que sont les services cloud IaaS, voire PaaS, serveurs, stockage et réseaux ne sont pas inclus dans le périmètre.

Le marché du PRA et DRaaS en France



D'ici 2028, le marché devrait augmenter de près de 35m€ par an et 137m€ au total.

Le segment des logiciels et appliances pesait 61% du marché total en 2024 et devrait représenter 57% des 766 m€ attendus en 2028.

Le marché du PRA et DRaaS en France

Ecosystème de fournisseurs de services sur le SMB

Rang	Société	Commentaires
1	ORANGE BUSINESS	Orange Business est considéré par Exaegis Markess comme un leader sur le marché du PRA et DRaaS en France sur le SMB.
2	CHEOPS TECHNOLOGY	Ex intégrateur qui a évolué vers les services à valeur ajoutée, l'infogérance, l'hébergement et le cloud, Cheops est très présent sur le stockage, la sauvegarde et le PRA. Son positionnement est focalisé sur le SMB régional.
3	ADISTA	Opérateur, prestataire d'hébergement, d'infogérance et de cybersécurité, Adista est présent sur l'ensemble du territoire et se concentre uniquement sur le SMB (en direct et en indirect). Sa stratégie est de proposer du one-stop-shop à ses 50 000 clients.
4	CYLLENE	Opérateur télécom, hébergeur et fournisseur de cloud privé, Cyllene dispose d'une forte expertise du stockage et propose des solutions de sauvegarde et reprise d'activité à sa large clientèle de SMB.
5	SIGMA	L'hébergeur et fournisseur de cloud nantais adresse une clientèle mid-market et possède des atouts sur les services de sauvegarde et PRA, en particulier dans environnements IBM.
6	IBM	IBM reste un fournisseur majeur du marché, en particulier autour de sa gamme iSeries
7	HARDIS	A la fois éditeur et expert des services numériques pour les secteurs logistique, distribution et finance, Hardis propose toute une gamme de services dont le PRA.
8	FREE PRO	Free Pro propose des services de cloud et d'hébergement robuste, dont la sauvegarde et le PRA sont un des socles.
9	ANTEMETA	Leader indépendant du marché du stockage avec plus de 100 m€ de CA, Antemeta a développé des expertises sur la data-résilience et la cyber-sécurité.
10	CLARANET	Claranet est un leader de l'infogérance hybride et multicloud et adresse le haut du mid-market avec des offres de conseil et infogérance adaptée, dont la continuité d'activité.

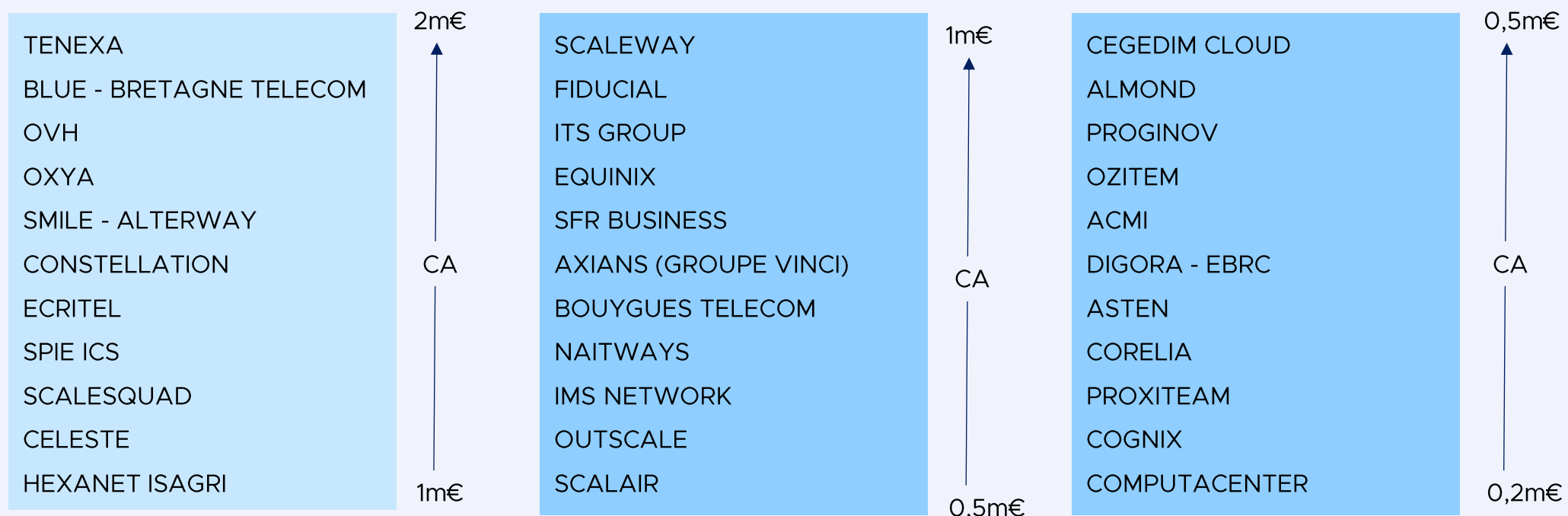
10m€

CA PRA

2m€

Le marché du PRA et DRaaS en France

Ecosystème de fournisseurs de services sur le SMB



Le marché des services liés au PRA et DRaaS est extrêmement fragmenté et près de 60 sociétés y ont une activité significative

02

Les enjeux de sauvegarde et continuité d'activité

Enjeux, moteurs et freins à la demande

Les enjeux de sauvegarde et continuité d'activité

Une pression réglementaire croissante qui accélère la demande de solutions de cyber-résilience souveraines :

Cyber Résilience Act (UE) Application début 2027	DORA (UE) Application au 17 janvier 2025	NIS 2 (UE) Transposition nationale en octobre 2024
Concernés : Fabricants de produits numériques (IoT, logiciels, plateformes) Exigences clés sur PRA / sauvegarde / résilience • Résilience « by design » • Mise à jour de sécurité durant tout le cycle de vie • Évaluation de l'impact d'un défaut sur la continuité	Concernés : Banque, assurance, fintech, prestataires IT critiques Exigences clés sur PRA / sauvegarde / résilience • PRA/PCA documenté et testé annuellement • Résilience des SI critiques • Journalisation et auditabilité • Gestion des tiers (contrats, SLA, réversibilité)	Concernés : Opérateurs de services essentiels et importants (OES/OIS) dans 18 secteurs comprenant 15 000 entités en France et plus de 180 000 en Europe. Exigences clés sur PRA / sauvegarde / résilience • Mise en place d'un PCA/PRA testé régulièrement • Sauvegarde sécurisée et restaurable • Obligations sur la supply chain IT

Contexte, le marché du cloud auprès du mid-market

Tendances :

Les entreprises adoptent de plus en plus des **solutions de sauvegarde hybrides**, qui combinent les avantages des environnements locaux et du cloud pour améliorer la protection des données et la flexibilité opérationnelle. Ces modèles hybrides permettent de concilier rentabilité, contrôle et évolutivité, tout en assurant un accès rapide aux données critiques en cas d'urgence.

Une autre tendance majeure est **l'intégration de l'IA et du machine learning** dans les systèmes de sauvegarde. Ces technologies permettent la détection des anomalies, la maintenance prédictive et l'automatisation des workflows de restauration, réduisant ainsi les objectifs de temps de restauration (RTO) et les objectifs de point de restauration (RPO).

La protection continue des données (CDP) devient également essentielle pour minimiser les pertes de données et assurer une continuité d'activité transparente. La complexité croissante des infrastructures modernes, notamment avec le multicloud et l'IoT, pousse les éditeurs à développer des solutions de sauvegarde plus polyvalentes et interopérables.

Enfin, il y a aujourd'hui une demande croissante pour des **sauvegardes immuables** et la vérification de l'intégrité avec la blockchain pour lutter contre les menaces cyber et garantir des enregistrements de données inviolables.

Défis :

La complexité de gestion et d'intégration des solutions dans des environnements informatiques variés, hybrides et multicloud, reste complexe. Cela peut engendrer des erreurs en matière de protection des données et une inefficacité des

processus de sauvegarde. **Le shadow IT**, les solutions SaaS utilisées par des départements sans connaissance par l'IT participe à la complexité.

Le marché des logiciels de PRA reste extrêmement fragmenté et il est **compliqué pour un décideur de faire un choix** entre des solutions sur site, cloud ou hybrides, chacune offrant ses avantages spécifiques en termes de contrôle, d'évolutivité et de coût. Les types de sauvegarde incluent la sauvegarde complète, incrémentielle, différentielle et la protection continue des données (CDP), permettant aux entreprises de choisir des stratégies optimales en fonction de leurs objectifs de restauration et de la fréquence de modification des données. **Cette variété de solutions nécessite un accompagnement et du conseil.**

Les ransomware modernes ciblent directement les sauvegardes. Assurer la sécurité, l'immuabilité et l'isolation des données de sauvegarde devient une priorité. De plus, la réglementation en matière de confidentialité des données ajoute une couche supplémentaire de complexité, en particulier pour les multinationales devant se conformer à des législations variées.

Les solutions de stockage proposent du stockage sur disque, sur bande, cloud et hybrides, avec des performances en vitesse, en coût et en durabilité variables. Selon les secteurs / métiers (santé, finance, industrie, distribution, etc) et les réglementations, les choix technologiques ne seront pas les mêmes. **Des configurations types peuvent être définies et proposées par les intégrateurs.**

Enfin, **le marché est très varié selon la taille des organisations clientes**, entre des PME et des grandes organisations, nécessitant des solutions de sauvegarde adaptées en raison de leurs contraintes budgétaires et des infrastructures informatiques très différentes.

Les enjeux de sauvegarde et continuité d'activité

Les moteurs de la croissance

- 1 La **croissance exponentielle du volume de données** générées par les entreprises
- 2 La **multiplication (connue) des rançongiciels et des cybermenaces** sophistiquées accroît le besoin de solutions de sauvegarde fiables, garantissant une restauration rapide des données et minimisant les temps d'arrêt.
- 3 L'évolution de la demande pour **mieux gérer les environnements hybrides et multicloud**. Les entreprises recherchent des solutions de restauration évolutives, économiques et flexibles, capables de s'adapter aux différents environnements
- 4 L'**intégration de l'IA** dans les solutions SaaS permet l'analyse prédictive et la détection automatisée des menaces. Ces solutions permettent d'automatiser des workflows complexes, de détecter des anomalies, des temps de restauration plus rapides et une optimisation des ressources
- 5 Les **exigences de conformité réglementaire** et les lois sur la souveraineté des données poussent les entreprises à adopter des stratégies de sauvegarde robustes, pour minimiser les risques de pertes de données, l'impact des attaques par rançongiciel ou simples pannes système

6 Le **développement des objets connectés** et de l'analyse des données produites augmente la quantité de données produites à sauvegarder et la difficulté à les traiter (temps réel, technologies très variées nécessitant des stratégies de restauration plus sophistiquées et décentralisées)

7 Les **progrès des solutions de PRA** avec le cloud, l'automatisation pilotée par l'IA et une cybersécurité renforcée incitent les entreprises à adopter de nouveaux systèmes de sauvegarde, plus robustes et plus agiles

Le PRA n'est plus vu comme une simple "copie d'infrastructure" mais comme un vecteur de continuité métier et de réponse aux incidents

Besoin croissant d'intégration PRA – sauvegarde – SOC dans une **logique de data-résilience unifiée**.

Les enjeux de sauvegarde et continuité d'activité

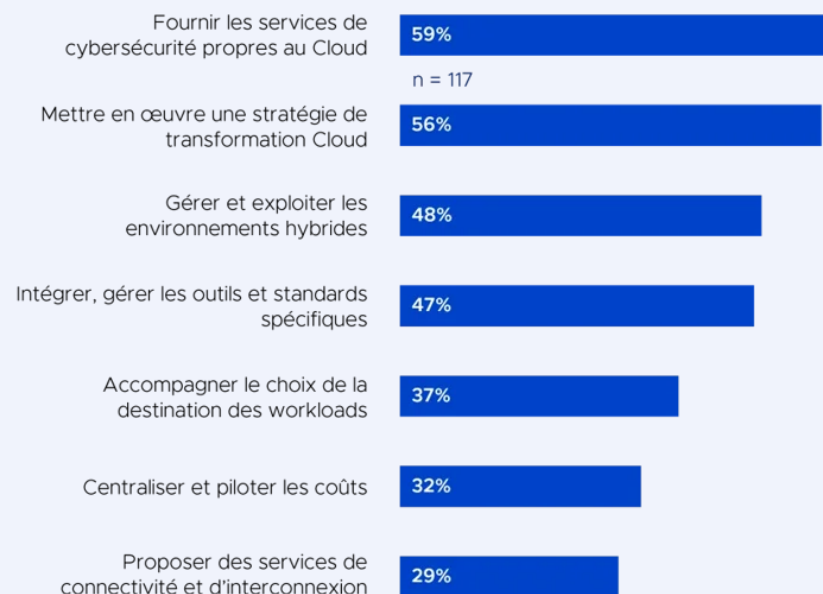
Enseignements pour Orange Business : se positionner en partenaire de confiance pour la gestion des infrastructures, dont le PRA et la cybersécurité

Le modèle hybride et multicloud s'impose et devient la norme pour la transformation digitale des organisations. Il impose aux prestataires de services cloud (Cloud MSP) de proposer, outre les services de gestion opérationnelle, des services d'accompagnement à la planification et la conception du cloud ainsi que des services de cybersécurité. Dans ce sens, Orange Business peut se positionner en tant que partenaire de confiance de l'organisation cliente.

Orange Business peut être le gestionnaire global et agnostique d'une informatique de plus en plus hétérogène, avec des capacités à délivrer des services de conseil et de gouvernance de la conformité.

La complexité, le besoin d'interopérabilité et de gestion inter-environnements incitent les petites et moyennes organisations à s'appuyer sur un prestataire à même de les accompagner dans la durée.

Le choix d'un prestataire pour vous accompagner dans votre stratégie de Cloud hybride repose sur ses capacités à :



© Markess by Exaegis, 2024

03

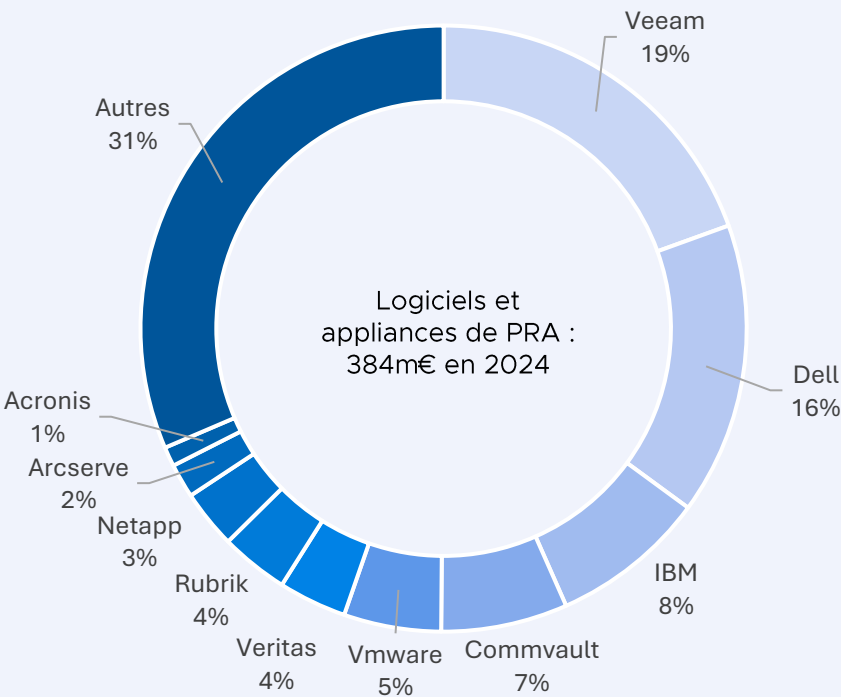
Les solutions de sauvegarde et PRA

Solutions commerciales et opensource

Les solutions de sauvegarde et PRA

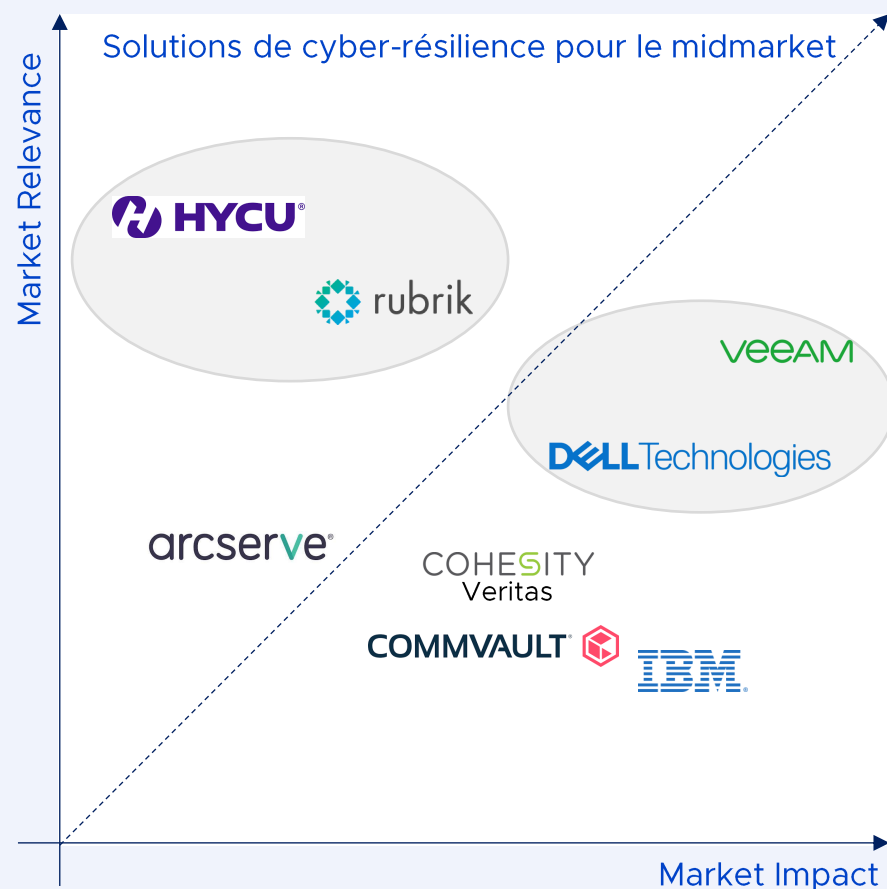
Classement des solutions commerciales selon leur chiffre d'affaires

Rang	sociétés	2023	2024	24/23	Market share
1	Veeam	65	75	15,4%	19,5%
2	Dell	60	60	0,0%	15,6%
3	IBM	33	32	-3,0%	8,3%
4	Commvault	26	26	0,0%	6,8%
5	Vmware	19	20	5,3%	5,2%
6	Veritas (Cohesity)	15	14	-6,7%	3,6%
7	Rubrik	12	14	16,7%	3,6%
8	Netapp	12	12	4,3%	3,1%
9	Arcserve	7	7	0,0%	1,8%
10	Acronis	4	4	14,3%	1,0%
Top 10		252	264	+4,8%	
Représentativité		68,1%	68,8%		
Marché		370	384	+3,8%	



Les solutions de sauvegarde et PRA

Positionnement des sociétés



Les solutions commerciales de cyber résilience qui sont recommandées à ce stade de l'analyse pour le développement sur le mid-market sont Veeam, Rubrik et Dell.

HYCU est également un bon candidat avec une solution jugée très pertinente mais ne semble pas avoir de présence en France.

Au-delà, des solutions open source sont présentes sur le marché et peuvent soutenir la technologie d'un MSP :

- [Restic](#) : une solution développée depuis 2014 se voulant simple (en ligne de commande), rapide, fiable et sécurisée disposant d'une large communauté.
- [Plakar](#) : une jeune solution open source développée en France depuis 2024 souhaitant proposer une efficacité et une fiabilité augmentée.

Les solutions de sauvegarde et PRA

Analyse des fournisseurs

		
Veeam est devenu leader du marché français en affichant une solide croissance ces dernières années, en particulier auprès du midmarket. La société propose dans sa gamme Veeam Data Platform, Veeam Data Cloud et des solutions communautaires gratuites pour Azure, Google Cloud, AWS et Kubernetes. La clientèle de Veeam est très large, avec des clients grands comptes, de taille intermédiaire et PME.	Rubrik propose un catalogue de solutions pour la data-protection (dont Rubrik Security Cloud), cyber-posture, l'analyse des menaces et la cyber-recovery. La société propose des solutions de protection des données sur site avec des appliances et dans le cloud. La clientèle comprend des ETI et grands comptes d'Amérique du Nord et d'Europe. Rubrik Security Cloud se veut être la première solution Zero Trust design and alimentée par l'IA.	Le constructeur et éditeur IBM se concentre désormais sur la sécurité des données et les services cloud. Il propose une gamme de solutions comprenant notamment IBM Storage Protect et IBM Storage Protect for Cloud pour les SaaS ainsi que Storage Defender. Ces solutions peuvent être combinées à l'offre de sécurité des données IBM Guardium. IBM couvre le monde entier et possède une clientèle allant de la PME aux plus grands comptes.
• Un rythme d'innovation intense avec de nouvelles fonctionnalités comme la détection de logiciels malveillants en ligne, l'analyse de contenu et un assistant basé sur l'IA et une offre BaaS pour les clouds Microsoft • Format de données de sauvegarde auto-descriptif : Les solutions de sauvegarde de Veeam utilisent un fichier de données de sauvegarde auto-descriptif, permettant la portabilité des données. • Un réseau de partenaires MSP pour adresser le midmarket qui se densifie rapidement, en particulier sur le cloud privé • Une tarification attractive (390€/an pour 5 instances cloud)	• Rubrik propose un moteur de récupération proactif permettant des temps de reprise rapide • La solution Rubrik Security Cloud est jugée simple et efficace • Forte capacité d'innovation et développement d'outils d'IA générative pour faciliter la gestion de la sécurité et des opérations. Également, des fonctionnalités de surveillance des données et de leur sécurité basées sur la détection des anomalies et des menaces. Acquisition récente de Predibase, une solution de développement de LLM qui permettra à Rubrik d'augmenter encore sa proposition de valeur avec l'IA. • Une gamme de solutions spécifiquement structurées pour les contraintes sectorielles (santé, finance, secteur public,	• Support des environnements hybrides et multi-cloud • Des solutions de cyber-résilience et de protection des données robustes, de premier plan, avec un catalogue très vaste • Des investissements massifs dans l'IA pour améliorer la proactivité et la détection des menaces (analyses comportementales, détection des anomalies) • Des solutions très puissantes pour la sauvegarde et la récupération de conteneurs (Red Hat OpenShift et Kubernetes) • Un réseau de partenaires extrêmement étendu et adapté à toutes tailles d'organisations
• Les solutions proposées par Veeam paraissent moins innovantes et moins adaptées aux environnements cloud natifs IaaS, PaaS et SaaS que certaines (Rubrik, HYCU) • L'environnement de gestion de Veeam Backup & Recovery nécessite une infrastructure serveur Windows	• Les environnements cloud gérés par Rubrik sont limités à AWS, Google Cloud, Microsoft Azure, Salesforce et Jira. • Réseau de partenaires encore très limité en Europe et en France (Cyllene, Scasicomp, Tersedia, S-Cube).	• L'intégration des solutions est jugée complexe, en particulier pour les PME et petites ETI • Les solutions IBM sont parfaitement adaptées aux environnements IBM et RedHat, mais demanderont parfois d'être complétées par d'autres environnements. • Les solutions IBM Storage Defender utilise la solution de Cohesity Data Protect.

Les solutions de sauvegarde et PRA

Analyse des fournisseurs

		
HYCU R-Shield est une plateforme BaaS hybride et multicloud couvrant Azure, AWS et GCP, prenant en charge les charges de travail IaaS, DBaaS, PaaS, SaaS et sur site. La société propose également R-Graph pour la visualisation et le pilotage des opérations. Historiquement uniquement sur Nutanix, l'entreprise qui n'a que 7 ans a rapidement évolué et couvre désormais l'Amérique du Nord et l'Europe, dont la France depuis peu avec des partenaires comme Devoteam, SPIE ICS et Orange Business. Sa clientèle est principalement composée d'ETI.	Dell propose une suite de solutions de protection des données avec logiciels, appliances et solutions as-a-service dont notamment PowerProtect Data Manager, les appliances PowerProtect, PowerProtect Cyber Recovery, CyberSense, et APEX Backup Services. Le groupe est 2ème du marché en termes de CA en France et adresse autant les PME, les ETI que les grands comptes.	Commvault propose la plateforme de Commvault Cloud, comprenant des solutions de protection des données, d'analyse des risques et de cyber-résilience des environnements on-premise, cloud IaaS, PaaS et SaaS. La clientèle est essentiellement composée d'ETI et grands comptes.
• Une offre de cyber-résilience avec une très large couverture des environnements cloud, publics comme privés, en particulier sur le SaaS. • Une solution jugée très ergonomique et intuitive avec un support client de premier plan (NPS de 91), une approche par API avec la solution R-Graph permettant de connecter de nouveaux environnements rapidement. • Intégration de l'IA générative pour faciliter la protection des environnements SaaS et PaaS.	• Positionnement clair sur la cyber-résilience et l'amélioration de la protection des données multicloud, reposant sur l'IA avec des solutions de sauvegarde, de récupération et de rétention de bout en bout. • Une offre complète et intégrée de solutions « one-stop-shopping » comprenant logiciels on-premise et SaaS, appliances, serveurs, stockage et réseau • Des solutions adaptées aux clouds AWS, Microsoft et Google, à Kubernetes, au cloud privé VMware, aux postes de travail et NAS.	• Multi environnement : les solutions de Commvault couvrent tous les environnements applicatifs ; on-premise, cloud native IaaS et PaaS, Kubernetes, SaaS, cloud privé VMware, Nutanix et s'adaptent au cloud hybride. • Le discours et les solutions proposées sont concentrées sur la cyber-résilience des environnements multiples, l'avenir de la sauvegarde et du PRA. • Des solutions d'analyse de risque et d'identification des données sensibles, notamment basée sur l'IA (solution 'Arlie'). • La solution Commvault Cleanroom Recovery qui permet de créer un espace cloud pour tester les plans de reprise d'activité et restaurer un environnement en cas d'attaque ou de ransomware.
• Peu ou pas de gestion des environnements applicatifs legacy, non cloud et non virtualisés. • L'automatisation de la récupération après sinistre semble en retrait et non unifiée, gérée environnement par environnement.	• La protection des environnements SaaS est très limitée. • L'ouverture aux environnements cloud natifs est récente et les solutions Dell restent plus adaptées au cloud privé et on-premise. • Les développements produits récents portent essentiellement sur les solutions adaptées aux moyennes et grandes organisations, délaissant les PME avec des besoins simples mais fiables.	• Le service support de Commvault est jugé comme moins bon que d'autres acteurs, en particulier en termes de réactivité • Malgré une communauté développée, le self service, la documentation et les tutoriels semblent faire défaut et les clients doivent souvent faire appel aux partenaires

Les solutions de sauvegarde et PRA

Analyse des fournisseurs

COHESITY	arcserve®
Cohesity propose un large portefeuille de solutions de cyber-résilience dont DataProtect, Netbackup (ex Veritas) qui sont disponibles on-premise, dans le cloud et en mode SaaS. Les développements majeurs incluent Cohesity Gaia, une solution de recherche et de réponse conversationnelle basée sur l'IA générative, alimentée par des données sauvegardées des clients. L'éditeur utilise également l'IA pour améliorer la détection des menaces et aider les gestionnaires de backup à améliorer la cyber-résilience. La clientèle de Cohesity est principalement constituée de grands comptes et grandes ETI, en Amérique du Nord et en Europe.	Arcserve propose un portefeuille de solutions comprenant Backup, Unified Data Protection, UDP Cloud Hybrid, les appliances Arcserve 9000 Series, les appliances de stockage Arcserve OneXafe et Arcserve SaaS Backup. Arcserve adresse des organisations de taille intermédiaire à grande dans le monde entier. La nouvelle solution Arcserve Unified Data Protection 10, propose une cyber-résilience renforcée avec des sauvegardes cohérentes et immutables, gérées depuis une interface intuitive unique. Elle propose également une gestion de la sécurité des mots de passe améliorée, la compatibilité avec de nouvelles distributions Linux, des correctifs de sécurité et une sécurité renforcée pour l'utilisation de la base de données SQL Express.
• Une marketplace qui propose des applications du groupe comme des solutions tierces pour mieux automatiser, améliorer, sécuriser les données des entreprises. • Cohesity possède de fortes capacités d'innovation en matière de protection des données et cyber-résilience, avec une roadmap cohérente. • Cohesity est un pionnier dans l'utilisation de l'IA générative entraînée sur les données des entreprises	• Options de tarification flexibles : Arcserve propose des licences on-premise perpétuelles et des licences SaaS associées à des métriques permettant d'optimiser les coûts. • Couverture géographique : Arcserve combine gestionnaires de territoire, revendeurs à valeur ajoutée (VAR) et fournisseurs de services gérés (MSP) dans toutes les grandes régions. • Protection complète des applications SaaS : Grâce à un partenariat avec Keepit, Arcserve SaaS Backup gère entre autres les environnements Microsoft 365, Salesforce, Google Workspace.
• L'intégration de Veritas reste encours (6 mois après son acquisition) et freine le rythme d'innovation du groupe. • En dehors des environnements cloud de Microsoft, SAP Hana et Salesforce, la couverture des applications SaaS reste limitée. • Cohesity ne proposait pas de solution de backup seule avant les acquisitions de Netbackup et Alta Recovery Vault. Ces acquisitions sont récentes, il faut attendre de voir comment elles vont s'intégrer fonctionnellement.	• Utilisation encore limitée de l'IA : Le portefeuille d'Arcserve manque d'implémentation de l'IA dans des domaines comme la détection d'anomalies. • Les investissements réalisés pour améliorer le support client et fiabiliser les solutions ont limité la capacité d'innovation de la société. • Les solutions proposées par Arcserve pour la sauvegarde des environnements de cloud public nécessitent l'installation et la gestion d'agent dédiés, ce qui complexifie la gestion de la solution dans ces environnements.

© 2025 Markess International SAS. et/ou ses sociétés sœurs ou mères. Tous droits réservés. Exaegis Markess est une marque déposée de Markess International SAS. et de ses sociétés sœurs et mères. Cette publication ne peut être reproduite ou distribuée sous quelque forme que ce soit sans l'autorisation écrite préalable d'Exaegis Markess. Elle comprend des analyses et des opinions issues de la recherche d'Exaegis Markess, qui ne peuvent être interprétées comme des déclarations de fait. Exaegis Markess décline toute garantie quant à l'exactitude, l'exhaustivité ou l'adéquation de ces informations. Les recherches d'Exaegis Markess peuvent aborder des sujets juridiques et financiers, néanmoins, Exaegis Markess ne saurait fournir de conseils juridiques ou financiers et ses analyses ou recherches ne doivent pas être interprétées ou utilisées comme telles. Votre accès et votre utilisation de cette publication sont régis par la politique d'utilisation d'Exaegis Markess. Exaegis Markess est particulièrement soucieux de sa réputation d'indépendance et d'objectivité. Ses analyses et recherches sont produites de manière indépendante par son équipe d'analystes de recherche, sans contribution ni influence d'une tierce partie.

exaegis.
markess

