



sonio.

Plus de clouds. Plus de liberté.

Et qui gère tout cela ?

Le cloud hybride comme modèle
d'exploitation : ce que les
consommateurs y gagnent et ce que
les opérateurs doivent assumer.

Le cloud ne commence pas au centre de données.

Tout environnement virtualisé n'est pas pour autant un cloud. Ce qui compte, ce sont l'automatisation, l'évolutivité, la transparence et la gouvernance.

Avant d'aborder le cloud hybride, il faut répondre en toute honnêteté à une question simple : qu'est-ce que le cloud, au juste ? La réponse est moins évidente que beaucoup ne le pensent.

Conclusion : la virtualisation est une base, pas un cloud. Quiconque continue à provisionner, à dimensionner et à facturer manuellement ses ressources n'exploite pas de cloud – même s'il utilise ce terme.

Et ceux qui parlent de « cloud » mais demandent de nouvelles machines virtuelles via un ticket entendent en réalité par là : un centre de données virtualisé sous un nom moderne.

Cloud hybride, multicloud, cloud de confiance : qu'est-ce que c'est ?

Le NIST distingue quatre modèles de déploiement : l'un d'entre eux – le « cloud privé » – est exploité

Nous nous basons sur la publication NIST SP 800-145, la définition internationalement reconnue. Cinq caractéristiques définissent le cloud :

CARACTÉRISTIQUE NIST	CE QUE CELA SIGNIFIE CONCRÈTEMENT
Libre-service à la demande	Des ressources disponibles à la demande – pas de ticket, pas d'attente, pas de processus manuel.
Accès étendu au réseau	Services accessibles via des mécanismes réseau standardisés – pas nécessairement via Internet.
Mise en commun des ressources	Ressources attribuées de manière dynamique à partir de pools communs.
Élasticité rapide	Capacité automatiquement évolutive – à la hausse comme à la baisse.
Service mesuré	L'utilisation est mesurée, rendue transparente et facturée.

Source : NIST SP 800-145, « The NIST Definition of Cloud Computing »

exclusivement pour une organisation, soit en interne, soit par un tiers. Un « cloud communautaire » partage l'infrastructure entre des organisations ayant des besoins communs (par exemple, des administrations ou des instituts de recherche). Un « cloud public » met des services à la disposition d'un large public via Internet. Enfin, le « **cloud hybride** » relie au moins deux de ces infrastructures cloud autonomes de manière à ce que les données ou les applications puissent être transférées entre elles. Cela nécessite une intégration, des normes et une

” Le cloud n'est pas un lieu. Le cloud, c'est la manière dont l'informatique est fournie et exploitée. Sonio SA, Pratique du cloud hybride

gouvernance commune. Ce livre blanc se concentre sur le « cloud privé », le « cloud public » et le « cloud hybride » – les modèles les plus pertinents pour les entreprises dans la pratique.

Le « **multicloud** » est un terme commercial désignant l'utilisation de plusieurs fournisseurs de cloud. Point essentiel : le multicloud n'implique pas automatiquement l'intégration. Celle-ci résulte souvent

de manière imprévue – du fait d'équipes, d'acquisitions ou de décisions individuelles. Utiliser plusieurs plateformes n'est pas un modèle d'exploitation. Les maîtriser, en revanche, en est un.

Le « **Trusted Cloud** » désigne des services cloud pour lesquels, outre la technologie, la juridiction, la conservation des données, la responsabilité opérationnelle, les sous-traitants, la sécurité, la transparence et les options de sortie peuvent être contrôlés de manière traçable. Le ministère fédéral de l'Économie et de la Protection du climat (BMWK) a forgé ce terme pour désigner un gage de qualité garantissant des services cloud sûrs et souverains (<https://trusted-cloud.de/ueber-trusted-cloud.html>). Le Sonio Cloud en est une illustration concrète.

LE CLOUD N'EST PAS UN LIEU.

L'« accès étendu au réseau » (Broad Network Access) désigne l'accès au réseau – pas nécessairement à Internet. Un cloud privé peut être entièrement exploité dans son propre centre de données tout en répondant aux cinq caractéristiques.

RÉSUMÉ

Le cloud hybride promet la liberté de choix : la liberté de placer les charges de travail là où elles sont le mieux gérées et de déployer des ressources plus rapidement que ne le permet une infrastructure classique. Ce que de nombreuses entreprises obtiennent en pratique : plus de plateformes, plus de règles, plus de charges d'exploitation – et au final, de nouveaux silos qui ne portent qu'un autre nom.

Le message clé est aussi simple que dérangeant : pour l'utilisateur final, le cloud hybride peut effectivement simplifier la vie. Pour l'opérateur, en revanche, cela devient nettement plus exigeant. La pression vient de deux côtés à la fois : les utilisateurs exigent plus de simplicité, plus de rapidité, de nouveaux services tels que l'IA. Dans le même temps, la menace s'aggrave et exige des réactions plus rapides, davantage de contrôle et une sécurité renforcée.

Ce livre blanc explique ce que signifie réellement le « cloud » selon le NIST, où réside la complexité du cloud hybride, quel rôle jouent l'IA, Kubernetes et la sécurité – et quelles capacités organisationnelles et quels modèles opérationnels permettent aux entreprises de réellement maîtriser tout cela.

Simple en façade. Complexe en coulisses.

Le cloud hybride masque la complexité pour le consommateur. Pour l'IT, les exigences augmentent en matière de plateforme, d'automatisation, de sécurité et d'exploitation.

Le consommateur ne veut ni cluster, ni VLAN, ni classe de stockage. Il veut un service. Rapide, sécurisé, sans ticket d'assistance. C'est le monde promis par le cloud hybride.

Cette simplicité pour l'utilisateur a un prix – et celui-ci n'est pas à sa charge. Les portails, les API et les workflows automatisés masquent la complexité technique. Derrière tout cela, quelqu'un doit la maîtriser : le service informatique, un partenaire de services managés ou une combinaison des deux. Calcul, stockage, réseau, identité, sécurité, coûts, cycle de vie, conformité : tout cela ne disparaît pas. Tout cela fait partie intégrante d'une plateforme. Et cette plateforme doit être construite, exploitée, sécurisée et développée par quelqu'un. Question : qui s'en charge dans votre organisation ?

73 % des organisations interrogées par Flexera en 2026 utilisent le cloud hybride, et 88 % font appel à plusieurs fournisseurs (Flexera, [State of the Cloud Report 2026](#)). La question n'est plus de savoir si les entreprises utilisent plusieurs plateformes. La question est de savoir si elles les maîtrisent réellement – ou si elles se sont simplement développées.

L'ingénierie des plateformes : ce qui se cache derrière

L'ingénierie des plateformes consiste à transformer la complexité en services réutilisables et standardisés. Un portail qui masque des processus manuels n'est pas un système en libre-service. Il s'agit d'un système de tickets informatiques doté d'une belle interface. Les véritables plateformes automatisent l'ensemble du cycle de vie : déploiement, exploitation, évolutivité, gestion du cycle de vie, reprise après sinistre. Ceux qui n'en sont pas capables ne disposent pas encore d'un cloud. Ils nourrissent simplement l'espoir d'y parvenir.

LA RÉALITÉ.

Pour l'utilisateur : ouvrir le portail, bénéficier du service, c'est tout. Pas de ticket, pas de temps d'attente.

Pour l'opérateur : les exigences en matière de plateforme, d'automatisation, de sécurité, de gouvernance et d'exploitation augmentent considérablement. Le cloud ne simplifie pas l'informatique. Il la rend plus exigeante.

Le contrôle ne va pas de soi.

Le cloud hybride exige des garde-fous clairs en matière de gouvernance, de souveraineté, de coûts et de sortie – sur l'ensemble des plateformes.

Exploiter plusieurs plateformes ne signifie pas automatiquement les maîtriser. La gouvernance ne commence pas par un ensemble de règles, mais par des lignes directrices communes qui s'appliquent à toutes les plateformes : identité, sécurité, journalisation, sauvegarde, classification des données, coûts, responsabilités. Celui qui invente ces lignes directrices séparément pour chaque plateforme ne construit pas un cloud hybride. Il construit plusieurs silos indépendants.

Souveraineté des données : l'emplacement du serveur ne suffit pas à lui seul

Un centre de données suisse évoque la sécurité.

Mais il ne la garantit pas automatiquement. Les éléments décisifs sont la juridiction, le chiffrement, les sous-traitants et la question de savoir qui peut exercer le contrôle en cas d'urgence. La Conférence des préposé(e)s suisses à la protection des données

(privatim) précise dans sa résolution de novembre 2025, adressée aux organes publics, que le Cloud Act américain peut également concerner des données hébergées dans des centres de données suisses – si le fournisseur est soumis au droit américain (privatim.ch, Résolution sur les solutions cloud internationales, 24 novembre 2025). L'emplacement des serveurs ne suffit pas à lui seul. C'est l'architecture juridique qui est déterminante. Pour les secteurs réglementés tels que la finance, l'industrie pharmaceutique ou le secteur public, il ne s'agit pas d'un débat abstrait sur la protection des données. Il s'agit d'une exigence de conformité qui influe directement sur le choix du modèle de cloud.

FinOps : des coûts du cloud à la valeur technologique

La question « Le cloud public est-il moins cher qu'un centre de données propre ? » est la mauvaise question en 2026. Le FinOps évolue d'une simple gestion des coûts du cloud vers la « valeur technologique » : 98 % des praticiens du FinOps gèrent déjà les dépenses liées à l'IA, 57 % le cloud privé et 48 % les coûts des centres de données (FinOps Foundation, State of FinOps 2026: data.finops.org). Ce qui compte, c'est de savoir quelle plateforme offre la meilleure valeur pour cette charge de travail – en termes de coûts, de risques, de performances, de souveraineté et de charges d'exploitation combinés.

UNE QUESTION ESSENTIELLE À SE POSER AVANT TOUTE ADOPTION DU CLOUD.

Comment en sortir ? Une stratégie de sortie doit être envisagée dès le début d'une décision relative au cloud, et non à la fin. Les données, les configurations, les identités, les interfaces et le savoir-faire opérationnel doivent rester transférables – sinon, on n'achète pas du cloud, mais de la dépendance.



Nouvelles charges de travail.

Même question de fond. L'IA et Kubernetes transforment les exigences du cloud hybride – pas ses principes fondamentaux.

Ceux qui pensent que le cloud hybride est un simple exercice d'infrastructure négligent deux évolutions qui en modifient fondamentalement la nature.

Kubernetes est devenu la couche opérationnelle standardisée pour les applications modernes. Selon l'enquête annuelle 2025 de la CNCF sur le cloud natif, 82 % des utilisateurs de conteneurs exploitent Kubernetes en production ; 66 % des organisations hébergeant des modèles d'IA générative utilisent Kubernetes pour les charges de travail d'inférence. Kubernetes est en soi déjà multicloud : les microservices proviennent de différentes sources, les frontières entre les infrastructures s'estompent.

L'infrastructure d'IA suit les mêmes principes que n'importe quelle autre infrastructure : où doivent résider et s'exécuter les données, les modèles et les ressources GPU ? La réponse dépend de la charge de travail, de la latence, des coûts, de la sécurité et de la souveraineté des données – les mêmes critères qui s'appliquent à toute autre charge de travail.

Ce qui vaut au niveau du CPU vaut tout autant au niveau du GPU. Il en découle qu'une architecture de cloud hybride qui ne peut pas également prendre en charge les charges de travail d'IA et de conteneurs n'est pas une architecture de cloud hybride pérenne. Elle représente l'avant-dernière étape.

LA PROCHAINE ERREUR EST PRÉVISIBLE.

Quiconque met en place l'IA comme une plateforme spécialisée isolée répète exactement l'erreur que le cloud hybride est censé résoudre : un nouveau silo, une infrastructure propre, une gouvernance propre, une exploitation propre. La préparation à l'IA ne commence pas par l'outil d'IA. Elle commence par la capacité à gérer conjointement la plateforme, les données, la sécurité et le cycle de vie.

La sécurité doit être plus rapide que l'attaque.

L'automatisation, la standardisation et le contrôle centralisé deviennent des exigences de sécurité – à travers le cloud, Kubernetes et l'IA.

L'IA n'accélère pas seulement les processus métier. Elle accélère également les attaques. Alors que les organisations utilisent l'IA pour gagner en efficacité, les attaquants exploitent cette même technologie pour identifier plus rapidement les surfaces d'attaque, exploiter automatiquement les vulnérabilités et faire évoluer leurs campagnes à grande échelle. La pression vient des deux côtés simultanément : l'entrepris exige de la rapidité. Le contexte de menaces laisse de moins en moins de temps pour réagir.

Au cours du deuxième semestre 2025, l'OFCS a reçu 29 006 déclarations volontaires et 145 déclarations

LES « CORRECTIFS INSTANTANÉS » COMME EXIGENCE DE LA PLATEFORME.

Les correctifs critiques doivent pouvoir être déployés rapidement grâce à des processus standardisés, automatisés et testés – et être tout aussi rapidement annulés. Le déploiement et la réversion sont des capacités inhérentes à la plateforme. Ceux qui les traitent comme des projets spécifiques n'ont pas encore compris l'exigence architecturale.

LE TEST DE SÉCURITÉ.

Si une vulnérabilité critique est exploitée plus rapidement que votre processus de changement ne peut déployer le correctif, vous n'avez pas seulement un problème de correctifs. Il s'agit avant tout d'un problème organisationnel : des processus trop lents, un manque d'automatisation, trop d'obstacles manuels. Et ce problème organisationnel a une conséquence architecturale directe : une plateforme incapable de déployer des correctifs rapidement et de manière contrôlée n'est pas une plateforme sécurisée.

obligatoires (OFCS, [rapport semestriel 2025/2](#)). Les ransomwares restent prédominants. Le phishing, l'usurpation d'identité et les attaques visant les chaînes d'approvisionnement logicielles deviennent plus ciblées et plus complexes. Le changement décisif ne réside pas dans le nombre d'attaques, mais dans leur rapidité.

Déployer des produits de sécurité au cas par cas ne résout pas le problème. Sécuriser séparément le cloud privé, le cloud public, Kubernetes et l'IA revient à exploiter plusieurs modèles de sécurité sans vue d'ensemble commune. La sécurité doit faire partie intégrante de l'architecture de la plateforme :

bases de référence standardisées, droits minimaux, segmentation, « policy-as-code », télémétrie centralisée et reprise testée.

” Quand le correctif est plus lent que l’attaque, ce n’est pas seulement la technique qui est trop lente.

Sonio SA, Pratique du cloud hybride

Plus une plateforme est construite de manière homogène, plus il est possible d’évaluer rapidement les vulnérabilités, d’appliquer les politiques et de

détecter les écarts. La standardisation n’est pas seulement une question d’efficacité : c’est un contrôle de sécurité.

Les agents IA constituent une nouvelle catégorie : il ne s’agit pas simplement d’un outil de plus, mais d’identités numériques dotées d’un pouvoir d’action. Quiconque est autorisé à lire, à prendre des décisions et à agir via des API doit être soumis à des restrictions, surveillé et contrôlable lors d’actions critiques. L’OWASP recense des incidents réels. Le NIST précise que les principes éprouvés de cybersécurité restent valables, mais doivent être systématiquement étendus aux agents autonomes.

Trois niveaux de menace auxquels les architectures de plateforme doivent être préparées :

PRIORITÉ	MENACE	CE QUE LA PLATEFORME DOIT ÊTRE CAPABLE DE FAIRE
Critique	Vulnérabilités, usurpation d’identité, ransomware	Règles de base standardisées, correctifs instantanés, droits d’accès minimaux, segmentation, procédure de reprise testée
Complexe	API, configurations cloud, chaîne d’approvisionnement logicielle et IA	Politiques sous forme de code, visibilité des dépendances, télémétrie centralisée, détection et réponse
Émergent	Injection de prompts, détournement d’agents, abus de privilèges par des agents IA	Identities d’agents distinctes, droits limités, portes d’approbation, tests continus

Sources : Rapport semestriel OFCS 2025/2 ; OWASP GenAI Exploit Round-up T1 2026 ; NIST, Security Considerations for AI Agents, mai 2026



C'est le workload qui décide.

Toutes les applications n'ont pas leur place dans le même cloud.

Il n'existe pas de cloud universellement idéal. Un service web mondial n'a pas les mêmes exigences qu'une application métier soumise à des obligations de conformité, qu'un cluster de GPU dédié à l'IA ou qu'un système d'archivage avec de longues durées de conservation. Prendre une décision concernant

le cloud avant d'avoir analysé la charge de travail revient à se tromper – et à en payer le prix plus tard sous forme de coûts de sortie de données, d'efforts de migration ou de dépendance vis-à-vis d'un fournisseur.

» Ce n'est pas le « Cloud First » qui mène à la bonne décision. C'est le « Workload First ».

Sonio SA, Pratique du cloud hybride

Six questions auxquelles il faut répondre avant toute décision concernant une charge de travail :

- **Données et conformité** : quelles données sont traitées ? Quelles sont les règles applicables – nLPD, FINMA, RGPD, règles spécifiques au secteur ?

Pour le placement des charges de travail, nous utilisons trois catégories – il ne s'agit pas d'une taxonomie NIST alternative, mais d'une classification axée sur la pratique :

CLOUD PRIVÉ	CLOUD DE CONFIANCE	CLOUD PUBLIC
Contrôle et intégration maximaux	Caractéristiques du cloud, associées à une traçabilité, un cadre juridique et des services managés	Large gamme de services de plateforme et évolutivité mondiale
Charges de travail étroitement couplées, stables ou réglementées	Lorsque souveraineté et allègement des opérations doivent aller de pair	Applications cloud natives, analytique et charge variable
L'exploitation reste exigeante : automatisation, sécurité et gestion du cycle de vie indispensables	La confiance repose sur l'espace juridique, la responsabilité, la transparence, la sécurité et la possibilité de se retirer – et pas uniquement sur l'emplacement du serveur	La gouvernance, le FinOps et la dépendance vis-à-vis des fournisseurs doivent être gérés de manière active

Remarque : Broadcom, les coûts liés aux hyperscalers et le Cloud Act sont des facteurs contextuels, et non une stratégie cloud. Il est possible de changer de fournisseur. La question du modèle d'exploitation adéquat reste posée.



- **Dépendances** : quels sont les liens techniques et organisationnels existants ? Qu'est-ce qui tourne sur quel hyperviseur ?
- **Performances et disponibilité** : quels SLA sont nécessaires – et peuvent-ils être mesurés et justifiés ?
- **Coûts totaux** : exploitation, licences, migration, trafic sortant, ressources humaines – calculés sur cinq ans, et non sur trois mois.
- **Sortie** : comment sortir de ce modèle – sur le plan technique, contractuel et opérationnel ?
- **Capacité opérationnelle** : notre organisation dispose-t-elle des compétences nécessaires pour assurer cette exploitation à long terme ?

Qui sait répondre à ces questions est prêt. Qui hésite a trouvé où agir.

UNE MACHINE VIRTUELLE PEUT ÊTRE DÉPLACÉE. UNE APPLICATION, PAS AUTOMATIQUEMENT.

Les applications dépendent de bases de données, de latences, d'interfaces, de licences, d'identités et de processus opérationnels. Ne pas connaître ces dépendances revient à prendre des décisions concernant le cloud à l'aveuglette – et on ne s'en rend compte que lorsque la migration coûte deux fois plus cher que prévu.

La technique ne suffit pas.

Le cloud hybride exige des processus, des compétences et des responsabilités adaptés.

Le cloud hybride ne transforme pas seulement l'infrastructure. Il modifie la manière dont l'informatique est organisée, dont les processus se déroulent et quelles compétences sont requises. Les services informatiques classiques sont structurés en fonction des technologies : équipe serveurs, équipe stockage, équipe réseau. Une organisation en plateforme nécessite autre chose : une responsabilité de plateforme transcendant les frontières entre domaines, un lien direct avec l'activité métier, une expertise en automatisation.

Quand l'automatisation s'arrête aux limites des processus

Un cas de figure typique tiré de la pratique : la plateforme peut provisionner une machine virtuelle en cinq minutes. Mais le processus de changement prend cinq jours. Résultat : l'automatisation existe, mais se heurte à un mur de tâches manuelles. Les processus ITIL restent importants, mais doivent s'adapter à une plateforme hautement automatisée. Ne pas faire évoluer en parallèle la gestion du changement, la gestion des incidents et la gestion de la configuration revient à freiner la plateforme avant même qu'elle ne puisse produire ses effets. Dans le même temps, la gestion des relations métier (Business Relationship Management) gagne en importance. Les équipes chargées des plateformes informatiques doivent comprendre de quels services l'entreprise a réellement besoin, comment ceux-ci sont utilisés – et où des améliorations s'imposent. Sinon, l'informatique optimise sa technologie, mais

« MAKE OR BUY » ? COMMENÇONS PAR POSER LA BONNE QUESTION.

Quelles sont les compétences qui différencient votre entreprise et doivent rester en interne ? Quels services peuvent être standardisés et donc externalisés ? Et quelle plateforme un partenaire peut-il exploiter de manière plus fiable, plus évolutive ou plus rentable – parce qu'il se consacre exclusivement à cela ?

pas la valeur apportée au client. Swiss IT Magazine décrit expressément la transformation vers le cloud à l'horizon 2026 comme une mission stratégique, organisationnelle, humaine et opérationnelle – et non pas uniquement technique.

La pénurie de main-d'œuvre qualifiée se heurte à une complexité croissante

Les spécialistes expérimentés quittent le marché – la génération des baby-boomers tire sa révérence. Parallèlement, de nouvelles compétences sont requises dans les domaines de l'automatisation, de Kubernetes, de l'ingénierie de la sécurité, des FinOps et des opérations d'IA. Ces deux phénomènes se produisent simultanément. Ceux qui pensent résoudre ce problème par de simples offres d'emploi sous-estiment le temps nécessaire à l'acquisition de ces compétences.

D'abord comprendre. Ensuite décider.

Sonio apporte de la transparence sur les workloads, les coûts, les risques et les modèles d'exploitation – avant que les décisions d'architecture ne soient prises.

Celui qui commence par un produit a déjà négligé la décision la plus importante. Une stratégie de cloud hybride solide commence par la transparence : sur les services métier, les applications, les données, les coûts, les risques et – évaluée en toute honnêteté – sa propre capacité opérationnelle.

L'évaluation du cloud hybride de Sonio n'est pas un outil commercial. Il s'agit d'une analyse structurée dont le résultat n'est pas une liste de produits, mais une cartographie des charges de travail, une vision cible pour le modèle d'exploitation et de sécurité, ainsi qu'une feuille de route réalisable.

Comment Sonio vous accompagne : trois modèles d'exploitation

- **Managed On Premises** : Sonio exploite les plateformes chez le client – surveillance,

sécurité, gestion du cycle de vie, application des correctifs.

- **Managed Sonio Cloud (Trusted Cloud)** : cloud suisse, exploité par Sonio – souveraineté des données, conformité et service géré par un seul et même prestataire.
- **Managed Hyperscaler** : gouvernance, FinOps, sécurité et exploitation sur Microsoft Azure – avec une répartition claire des responsabilités et une transparence totale.

L'architecture reste ainsi ouverte. Une charge de travail peut s'exécuter là où elle est le mieux prise en charge sur le plan technique – et non là où le prochain contrat a déjà été signé.

CE QUE FOURNIT L'ÉVALUATION DU CLOUD HYBRIDE

Carte des charges de travail : quelles sont les applications existantes ? Quelles sont leurs dépendances, leurs exigences de conformité et leur compatibilité avec le cloud ?

Transparence totale des coûts : coûts d'exploitation, risques liés aux licences, coûts de sortie de données et décisions « faire ou acheter » clairement exposés.

Placement des charges de travail : cloud privé, cloud de confiance ou cloud public – justifié, pas simplement vendu.

Recommandation de modèle d'exploitation : qu'est-ce que votre service informatique gère en interne ? Qu'est-ce qui relève d'un service géré ? Une décision prise en toute connaissance de cause.

La simplicité n'est pas le fruit du hasard.

Le cloud hybride ne fonctionne que si la complexité est délibérément standardisée, automatisée et exploitée.

Le cloud hybride facilite la vie du consommateur. Mais seulement si quelqu'un se charge délibérément de standardiser, d'automatiser et de gérer la complexité qui se cache derrière. Cela ne se fait pas tout seul.

” Simple pour l'utilisateur signifie : rigoureusement conçu en coulisses.

Sonio SA, Pratique du cloud hybride

La question gestionnelle décisive n'est donc pas « cloud ou centre de données ? ». Elle est la suivante : quelle plateforme convient à quelle charge de travail ? Quelles capacités l'organisation souhaite-t-elle posséder ? Et quelle complexité souhaite-t-elle gérer elle-même à long terme ?

Les sept enseignements clés :

- **Le cloud est un modèle d'exploitation, pas un produit.** Quiconque provisionne encore ses ressources manuellement pratique la virtualisation – pas le cloud.
- **Le cloud hybride déplace la complexité.** Le consommateur en profite. L'opérateur assume davantage de responsabilités – et a besoin d'une plateforme, d'une automatisation et d'une gouvernance qui soutiennent cela.
- **Le multicloud se développe souvent de manière imprévue.** Utiliser plusieurs fournis-

seurs n'est pas un modèle d'exploitation. La gouvernance, l'intégration et les normes communes, elles, le sont.

- **La sécurité, c'est l'architecture de la plateforme.** Correctifs instantanés, « policy-as-code », reprise testée : ce ne sont pas des modules supplémentaires, mais des capacités fondamentales.
- **L'IA et Kubernetes font partie de l'équation.** Ceux qui mettent en place l'IA comme un nouveau silo répètent les mêmes erreurs. Nouvelles charges de travail, mêmes questions.
- **Priorité à la charge de travail, pas au cloud.** La plateforme suit la charge de travail – pas le fournisseur ni la tendance.
- **C'est l'organisation qui détermine le succès ou l'échec.** La technologie est rarement le principal problème. Ce sont les compétences, les processus et les décisions « faire ou acheter » qui comptent.

LA DÉCISION.

Si demain, un nouveau service métier, une charge de travail IA ou une exigence réglementaire vient s'ajouter : votre service informatique est-il capable de le déployer de manière contrôlée, sans créer un nouveau silo ? Si ce n'est pas le cas, c'est précisément là que le travail commence.

Passer à l'action.

Avec des vérifications claires, une vision fiable des workloads et un modèle d'exploitation adapté, le cloud hybride devient une feuille de route concrète.

Trois horizons temporels – des mesures concrètes pour les PME, les entreprises de taille intermédiaire et les grandes entreprises.

Mesures immédiates : cette semaine

1. Bilan de la situation dans le cloud : combien de temps faut-il pour déployer une nouvelle machine virtuelle ? S'agit-il d'un service en libre-service ou d'un processus de ticket ? La réponse vous indiquera où vous en êtes réellement.

2. Bilan Broadcom : quelles versions de VMware utilisez-vous ? Quand le contrat expire-t-il ? Fin du support général de vSphere 8 en octobre 2027 : si vous ne planifiez pas dès maintenant, vous devrez le faire sous pression.

3. Bilan de souveraineté : quelles données et applications sont hébergées chez des fournisseurs américains ? Quelles en sont concrètement les conséquences en matière de conformité ?

À moyen terme : au cours des 90 prochains jours

1. Inventaire des applications et des dépendances : qu'est-ce qui fonctionne ? Quelles sont les interdépendances ? Qu'est-ce qui est réellement compatible avec le cloud – et qu'est-ce qui ne l'est pas ?

2. Analyse des coûts globaux : exploitation, licences, trafic sortant, ressources humaines, cycle de vie – sur cinq ans, pas sur trois mois.

3. Lancer une évaluation du cloud hybride : avec un partenaire qui fournit une cartographie des charges de travail – et non une simple liste de produits.

Stratégie : votre feuille de route vers le cloud

1. Définir le modèle d'exploitation : qu'est-ce que votre service informatique gère en interne ? Qu'est-ce qui est souscrit en tant que service géré ? De manière réfléchie – et non pas par habitude historique.

2. La sécurité en tant qu'architecture de plateforme : correctifs instantanés, « policy-as-code », télémétrie centralisée, reprise testée – des capacités de la plateforme, pas des projets spécifiques.

3. Prévoir la préparation à l'IA et à Kubernetes : celui qui planifie la plateforme aujourd'hui participe à la décision – à savoir si, dans deux ans, les charges de travail d'IA et les services de conteneurs pourront être intégrés de manière pertinente.

4. Mettre en place le FinOps : rendre visibles les coûts et la valeur pour l'ensemble des plateformes – cloud privé, cloud de confiance, cloud public.

PRÊT POUR LA PROCHAINE ÉTAPE ?

Sonio vous accompagne de l'évaluation au placement des charges de travail, en passant par le service géré continu – sur les trois modèles d'exploitation. Quel que soit le cloud qui vous conviendra finalement.

**Prenez rendez-vous dès maintenant pour un
premier entretien sans engagement :**

www.sonio.com/hybrid-cloud

Source principale : table ronde sur le livre blanc consacré au cloud hybride avec Markus Fischer, Dirk Weis et Ralph Budil, Sonio AG, 3 août 2026.

Sources externes : NIST SP 800-145. Flexera State of the Cloud 2026 (73 % de cloud hybride, 88 % de multicloud). FinOps Foundation, « State of FinOps 2026 ». Enquête annuelle 2025 de la CNCF sur le cloud natif (82 % de Kubernetes en production, 66 % pour l'inférence GenAI). Rapport semestriel 2025/2 de l'OFCS (29 006 déclarations volontaires, 145 obligatoires). Résolution de privatiser sur les solutions cloud internationales, novembre 2025. Swiss IT Magazine « Cloud-Transformation » 2026/06 et interview du CIO du groupe Rapp 2026/06. OWASP « GenAI Exploit Round-up » T1 2026. NIST « Security Considerations for AI Agents », mai 2026. Sonio Managed Services : sonio.com/services/managed-services.



sonio.

Contactez-
nous pour un
entretien sans
engagement :

info@sonio.com

www.sonio.com