Microsoft

Microsoft Sovereign Cloud pour l'Europe

Octobre 2026

Avis

Ce livre blanc fournit un aperçu détaillé de Microsoft Sovereign Cloud, l'approche complète de Microsoft en matière de souveraineté numérique pour les gouvernements, les organisations du secteur public et les entreprises opérant dans des secteurs hautement réglementés ou critiques. Il explique la manière dont Microsoft assure la souveraineté grâce à l'architecture technique, à la gouvernance opérationnelle et aux engagements juridiques, sans fragmenter la plateforme cloud ni limiter l'accès à l'innovation.

Ce document s'adresse à des publics externes, notamment des clients, des régulateurs et des parties prenantes politiques. Il est fourni à titre informatif seulement et ne crée aucun engagement contractuel.

Sommaire

Introduction 04

Notre approche en matière de conception 05

- Cloud public souverain
- Cloud privé souverain
- Écosystème partenaire souverain

Les opérations de Microsoft en Europes 14

- Structure d’entité
- Gouvernance d’entreprise et contrôles d’accès
- Engagements juridiques et contractuels pour les demandes d’accès
- Sous-traitants et transparence

Concrétiser la souveraineté numérique 17

Introduction

Chez Microsoft, nous pensons que les clients ne devraient jamais avoir à choisir entre souveraineté, sécurité et innovation. Microsoft Sovereign Cloud est conçu comme un portefeuille complet offrant des contrôles souverains de premier plan dans le cadre de l'écosystème de cloud le public, de cloud privé et de partenaires qui comprend des clouds partenaires gérés au niveau national où les réglementations spécifiques aux pays exigent une propriété et un contrôle indépendants.

À mesure que le cloud computing, les données et l'intelligence artificielle deviennent des piliers de la compétitivité économique, des services publics et de la sécurité nationale, les gouvernements et les entreprises se concentrent de plus en plus sur les personnes qui contrôlent et accèdent à leur infrastructure numérique, leurs données et leurs systèmes critiques. Ce changement a placé la souveraineté numérique au premier plan de la prise de décisions stratégiques. À travers l'Europe, ces technologies sont désormais la base de tout, de l'administration publique et des soins de santé aux marchés financiers, à la fabrication et aux chaînes d'approvisionnement. Les questions de contrôle, de gouvernance et de cadres juridiques applicables relèvent donc désormais du conseil d'administration et du cabinet.

Microsoft offre une infrastructure **mondiale** sécurisée, résiliente et complète, couvrant plus de 80 régions de datacenters et exploitant plus de 500 datacenters à l'échelle mondiale, qui offre aux clients un continuum de contrôles souverains. Des contrôles intégrés à cette infrastructure permettent aux organisations d'appliquer le niveau de souveraineté approprié à chaque charge de travail, qu'il s'agisse d'environnements publics, hybrides, totalement déconnectés ou gouvernés localement, si nécessaire. En intégrant des protections à chaque couche du cloud, Microsoft permet à ses clients d'exécuter des charges de travail stratégiques en toute confiance, tout en leur offrant la maîtrise des données, des accès et des opérations afin de répondre aux exigences de sécurité et de conformité les plus strictes.

En s'appuyant sur plus de 40 ans d'histoire en tant qu'entreprise en Europe, Microsoft a réalisé des investissements soutenus et à long terme pour s'assurer que cette infrastructure mondiale soit construite, exploitée et gouvernée conformément aux valeurs, lois et attentes européennes. Ces **investissements** comprennent l'expansion continue des infrastructures cloud et d'IA à travers l'Union européenne et les États membres de l'AELE, ce qui renforce la résilience régionale, la capacité et la redondance tout en soutenant la croissance numérique et économique de l'Europe.

Parallèlement, l'Europe doit faire face à un paysage réglementaire en rapide évolution, à la montée des menaces cybernétiques et à une incertitude géopolitique accrue. Les organisations subissent une pression croissante pour innover de manière responsable en adoptant les technologies cloud et d'IA, tout en veillant à ce que leurs données, opérations et propriétés intellectuelles restent protégées par le droit européen. Ces pressions dépassent le secteur public et s'étendent aux opérateurs d'infrastructures critiques et aux secteurs fortement réglementés, y compris les services financiers, la santé, l'énergie, les télécommunications et la fabrication. Pour de nombreuses organisations, la souveraineté numérique n'est plus un concept théorique, mais constitue une exigence pratique que les fournisseurs de services cloud doivent respecter en matière de technologie, d'opérations et de gouvernance.

En avril 2025, nous avons réaffirmé et approfondi notre engagement à long terme envers l'Europe en annonçant nos **engagements numériques en Europe**, afin de renforcer et d'élargir un ensemble d'assurances juridiques, techniques et opérationnelles contraignantes, conçues spécifiquement pour tenir compte de ces préoccupations. Ces engagements s'appuient sur plus d'une décennie d'investissements dans la confidentialité, la sécurité, la conformité et la résilience, y compris la préparation au RGPD, des pratiques de transparence de longue date et le périmètre des données de l'UE pour le Microsoft Cloud. Ensemble, ces engagements reflètent le rôle de Microsoft en tant qu'infrastructure critique pour l'Europe et la responsabilité qui en découle d'opérer de manière à soutenir les cadres juridiques, les attentes réglementaires et les valeurs de l'Europe.

Microsoft Sovereign Cloud s'appuie sur ce socle en transformant l'envergure mondiale de Microsoft, ses investissements en Europe et les engagements numériques européens en fonctionnalités de souveraineté concrètes et configurables pour les clients. Plutôt que d'isoler les clients dans des environnements distincts ou à fonctionnalité réduite, nous offrons la souveraineté directement au sein du Microsoft Cloud grâce à des contrôles intégrés, des modèles de déploiement flexibles et des engagements juridiquement contraignants. Grâce à cette approche, les organisations peuvent satisfaire aux exigences de souveraineté en constante évolution, tout en continuant de bénéficier de la puissance, de la sécurité et de l'innovation du Microsoft Cloud, et en maintenant leur conformité, leur contrôle et leur confiance.

Les cinq points clés de ce livre blanc

1. **Vous n'êtes pas enfermé dans une approche unique**
   Choisissez des options de déploiement flexibles qui s'adaptent et évoluent au fil du temps.

2. **Choisir le cloud souverain ne signifie pas ralentir l'innovation**
   Utilisez le cloud moderne et l'IA à grande échelle tout en répondant à vos exigences – sans compromis sur la performance, les capacités, la vitesse

3. **La mise en œuvre est effectuée via des contrôles en couches**
   Protection assurée par des contrôles techniques, contractuels et opérationnels

4. **Le contrôle s'applique au niveau de la charge de travail**
   Des charges de travail et des locataires individuels peuvent être protégés, pas seulement des régions entières

5. **Il est soutenu par le droit et la gouvernance européens**
   Renforcé par des cadres juridiques, une surveillance et une responsabilisation

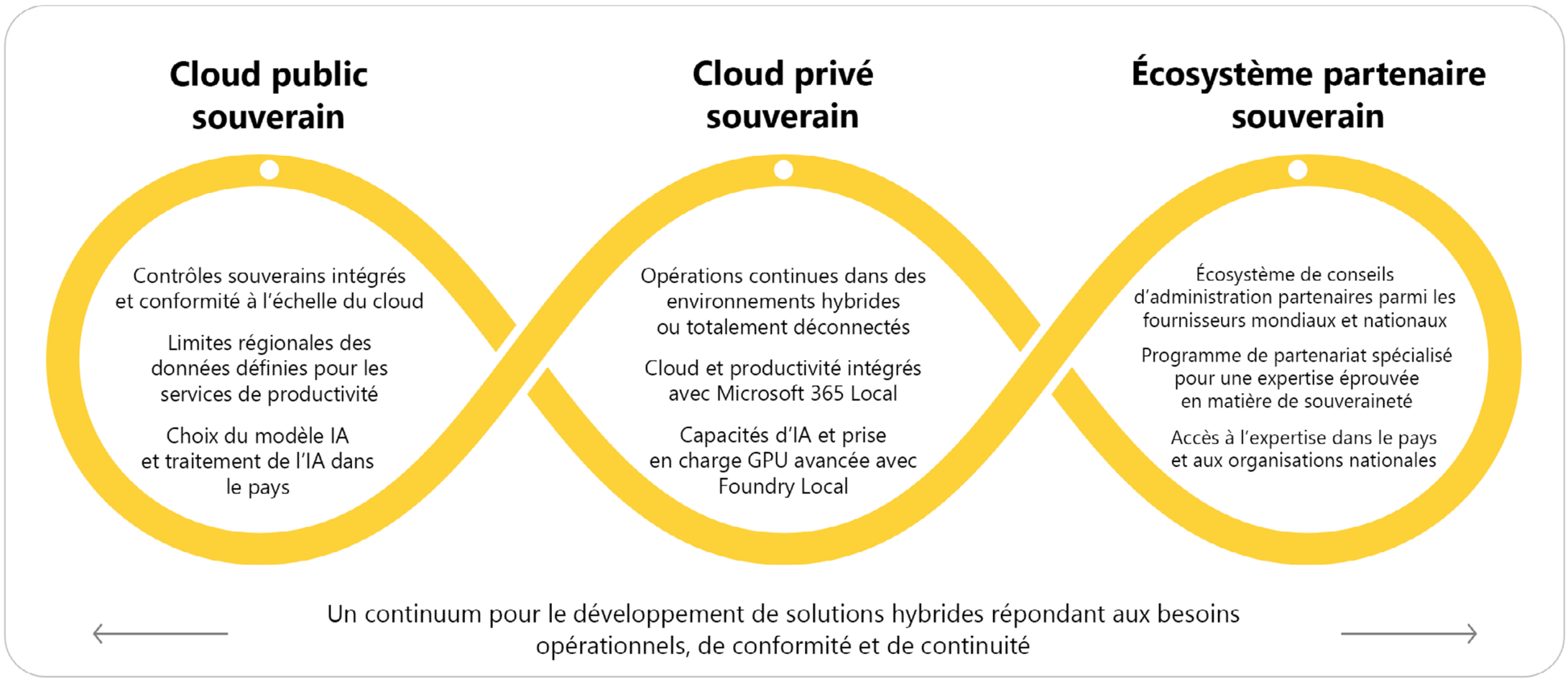
Notre approche en matière de conception

Notre approche est simple. La souveraineté est à la base de notre cloud et de nos services, assurée par une combinaison rigoureuse de contrôles techniques, contractuels et opérationnels. Dans la mesure où chaque charge de travail et chaque organisation présentent différents niveaux de sensibilité et de criticité, les exigences en matière de souveraineté sont adaptées aux besoins de chaque client.

Microsoft Sovereign Cloud réunit l'IA, la productivité, la sécurité et les charges de travail cloud pour couvrir les environnements publics, hybrides et déconnectés afin que les clients puissent appliquer le niveau approprié de contrôle, de fonctionnalité et de conformité en fonction de la sensibilité et de la criticité de chaque charge de travail, au lieu de dépendre d'un seul modèle de déploiement.

Microsoft Sovereign Cloud

La gamme de solutions de souveraineté la plus complète couvrant l'IA, la productivité, la sécurité et la plateforme cloud



Cloud public souverain

Fort de notre expérience dans la fourniture de solutions de souveraineté répondant aux besoins du secteur public et des clients hautement réglementés, notre cloud public souverain est le seul fournisseur de cloud qui offre des capacités complètes en matière d'IA, de productivité, de sécurité, et une plateforme cloud pour les clients européens dans l'ensemble de nos datacenters européens existants.

Avec le cloud public souverain, les données des clients (y compris celles traitées par des services d'IA, qu'elles soient au repos ou en transit) restent en Europe, en vertu de la législation européenne, avec des opérations et un accès contrôlés par du personnel européen, ainsi qu'un chiffrement entièrement sous le contrôle des clients. Ce paramètre est activé pour toutes les charges de travail client exécutées dans nos régions de datacenters européennes, **sans qu'aucune migration soit requise.** Les organisations n'ont pas à migrer vers un autre cloud, à redéfinir leurs environnements ni à modifier leurs architectures pour répondre à leurs exigences de souveraineté. Elles peuvent appliquer des contrôles souverains dans l'environnement qu'elles utilisent déjà.

Frontière des données de l'UE pour environnements de cloud public

Depuis 2023, Microsoft exploite une **frontière des données de l'UE** complète pour stocker et traiter les données clients de l'Union européenne (UE) et de l'Association européenne de libre-échange (AELE) en Europe, sauf lorsque les clients configurent explicitement les services autrement. Cet engagement vise à donner aux clients un contrôle clair sur l'emplacement des données tout en soutenant la conformité aux exigences de protection des données de l'UE et des États membres.

Dans le cadre de la frontière des données de l'UE, Microsoft conserve le contenu des clients, par exemple les fichiers, les e-mails, les documents et les données d'application, dans les datacenters de l'UE/AELE pour les services couverts tels que Microsoft 365, Azure, Dynamics 365 et Power Platform. Les clients conservent la capacité de configurer les mouvements de données ou d'activer des scénarios interrégionaux lorsque cela est nécessaire pour leurs opérations commerciales.

Outre le contenu des clients, la frontière des données de l'UE de Microsoft s'étend aux données générées par des services, y compris les données personnelles pseudonymisées, les journaux système, la télémétrie et les données de services professionnels générées lors des interactions avec le support. Avec l'achèvement de la phase finale de la frontière des données de l'UE, cette catégorie de données, souvent négligée dans les discussions sur la résidence, est également stockée au sein de l'UE/AELE pour les services concernés (cela n'inclut pas les données de facturation). Cela réduit les flux de données transfrontaliers et offre une posture de résidence plus complète que les modèles qui se concentrent uniquement sur les données créées par les clients.

Les engagements de Microsoft en matière de frontières des données incluent également le traitement de données par l'IA. Pour les services admissibles tels que Microsoft 365 Copilot, les requêtes et les réponses sont traitées au sein de la frontière des données de l'UE pour les clients qui résident au sein de l'UE/EFTA, et Microsoft développe des options nationales de traitement des données par l'IA afin de localiser davantage le traitement lorsque cela s'avère nécessaire.

Microsoft travaille en étroite collaboration avec les clients, les régulateurs et les autorités de protection des données afin de fournir une documentation claire, des rapports de transparence et des engagements contractuels décrivant les pratiques de gestion des données et les contrôles utilisés pour appliquer la frontière des données de l'UE. Cette approche permet aux clients d'évaluer et de démontrer la conformité tout en continuant de bénéficier de l'échelle, de la sécurité et des capacités d'innovation du Microsoft Sovereign Cloud.

Contrôles techniques

Microsoft met en œuvre des contrôles techniques de défense en profondeur qui réduisent la dépendance envers la fiabilité des opérateurs et offrent aux clients un contrôle de leurs données vérifiable et basé sur le chiffrement. Cela comprend :

Zone d'atterrissage souveraine (SLZ) pour une gouvernance et un déploiement axés sur les politiques

Créée sur la base de la zone d'atterrissage Azure (ALZ), la zone d'atterrissage souveraine fournit une architecture de référence prescriptive et évolutive, ainsi que des outils pour opérationnaliser la souveraineté numérique dans Azure. SLZ applique dès le départ les exigences de gouvernance et de conformité, avec les dernières mises à jour, notamment une hiérarchie des groupes d'administration améliorée et des définitions, initiatives et affectations intégrées d'Azure Policy, alignées sur les niveaux de contrôle du cloud public souverain. SLZ inclut des recommandations pour le déploiement de services clés, tels qu' Azure Key Vault Managed HSM le cas échéant, afin de permettre des niveaux plus élevés de contrôle souverain. Le déploiement est rationalisé grâce aux accélérateurs de zone d'atterrissage Azure, à l'infrastructure en tant que code (IaC) et aux bibliothèques réutilisables, ce qui permet aux organisations d'appliquer des contrôles de souveraineté de manière cohérente dans tous les environnements.

Isolation matérielle et protection des données en cours d'utilisation

Au niveau de l'infrastructure, Microsoft propose l'informatique confidentielle Azure, qui protège les données pendant leur traitement en exécutant les charges de travail à l'intérieur d'environnements d'exécution fiable (TEE) matériels. Ces environnements sont conçus de façon à ce que les données restent chiffrées en mémoire et inaccessibles aux opérateurs cloud, administrateurs ou autres processus logiciels à l'extérieur de l'enclave. Les clients peuvent utiliser l'attestation à distance pour valider l'intégrité de la pile matérielle et logicielle avant l'exécution des charges de travail afin de s'assurer que seuls les environnements de confiance peuvent traiter des données sensibles.

Contrôle du client de l'accès aux données par clé

Microsoft limite davantage l'accès grâce au chiffrement contrôlé par les clients. Avec les clés gérées par le client, Azure Key Vault Managed HSM et la gestion de clés externes, les clients gardent le contrôle des clés de chiffrement utilisées pour protéger leurs données. Dans la mesure où Microsoft ne possède pas ces clés, nous ne sommes pas en mesure de déchiffrer de manière autonome les données des clients. En cas de demande d'accès gouvernemental légal, toute donnée fournie restera chiffrée, la possibilité de les déverrouiller se trouvant entre les mains du client.

Supervision opérationnelle, visibilité et accès auditables

Pour les scénarios opérationnels où un accès limité est requis afin de maintenir la fiabilité du service, Microsoft applique des contrôles d'accès stricts avec visibilité par le client. La fonction Customer Lockbox nécessite une approbation explicite du client avant que le personnel de Microsoft puisse accéder au contenu client lors d'incidents de support. Pour les opérations souveraines européennes, Data Guardian ajoute la validation par un personnel européen et consigne toutes les actions d'accès privilégié dans des journaux infalsifiables, ce qui permet d'effectuer des examens post-événement et des audits réglementaires. Le Sovereign Control Panel fournit une expérience unifiée pour le pilotage et l'évaluation des contrôles de souveraineté et de la posture opérationnelle dans les environnements cloud. Les chemins d'accès sont authentifiés, autorisés et enregistrés, et les outils sont conçus pour que l'accès privilégié soit à la fois exceptionnel et traçable, plutôt qu'implicite.

Transparence et journalisation

Microsoft fournit des capacités complètes de journalisation et d'audit dans ses services cloud, permettant aux clients de surveiller les actions administratives, les tentatives d'accès et les opérations sur les données. Les dossiers d'audit sont protégés pour prévenir les modifications non autorisées et ils sont disponibles pour soutenir la gouvernance interne et les examens réglementaires externes. Les engagements contractuels de Microsoft viennent renforcer ces mesures techniques en exigeant la journalisation, la justification d'accès et la notification aux clients dans le cadre de ses contrôles opérationnels. Cela permet de s'assurer que les protections techniques sont complétées par des obligations exécutoires.

Feuille de route du cloud public souverain

Fonctionnalités améliorées du Sovereign Control Panel

Ces fonctionnalités permettront aux organisations de découvrir et de contrôler les exigences de souveraineté, et d'agir en conséquence grâce à une visibilité centralisée de la position de souveraineté, des contrôles de stratégie, de la gouvernance opérationnelle et du statut de conformité. De nouvelles capacités aideront les organisations à évaluer les exigences de souveraineté, à surveiller le respect des contrôles et à prendre des mesures dans les environnements cloud à partir d'une expérience unifiée.

Capacités étendues de calcul confidentiel pour le cloud public souverain

Ces capacités renforceront la protection des données en cours d'utilisation grâce à l'isolation matérielle et à des environnements d'exécution fiables, permettant ainsi à un plus large éventail de charges de travail sensibles dans le cloud et l'IA de bénéficier des protections du calcul confidentiel.

Capacités étendues de la zone d'atterrissage souveraine

Ces capacités intègrent la prise en charge de l'infrastructure en tant que code avec Bicep, ce qui permet aux organisations de déployer et d'exploiter des charges de travail souveraines à grande échelle grâce à l'application automatisée des politiques, des contrôles de gouvernance et des architectures conformes dès la conception. Cela permet d'accélérer le déploiement, de réduire la complexité de la conformité et de maintenir la visibilité sur la posture de souveraineté dans tous les environnements cloud.

Cloud privé souverain

Pour les clients dont les charges de travail présentent des besoins spécifiques, le cloud privé souverain apporte les services cloud, de productivité et d'IA de Microsoft dans des environnements détenus et exploités par le client. Azure Local constitue le socle de l'infrastructure, apportant les services Azure et une gestion cohérente avec le cloud aux environnements sur site et en périphérie. Les organisations peuvent ainsi exécuter localement des charges de travail virtualisées, des conteneurs et des services Azure tout en maintenant le contrôle opérationnel grâce à Azure Arc.

Sur cette base, les organisations exécutent les services Microsoft dont elles dépendent, complètement au sein de leur propre infrastructure. Les équipes utilisent des outils de productivité et de collaboration familiers avec Microsoft 365 Local et Azure Virtual Desktop. Les développeurs conçoivent et livrent des logiciels avec GitHub Enterprise Local, ce qui permet de conserver le code source et les workflows DevOps au sein de l'environnement souverain. Les données opérationnelles restent locales avec SQL Server et d'autres services de données relationnelles et documentaires. De plus, avec Foundry Local, les organisations exécutent des modèles IA, des outils et des agents directement sur ces données, ce qui signifie que les informations sensibles ne quittent jamais l'environnement souverain. Les clients exécutent leurs propres applications en parallèle de tout cela sur des machines virtuelles à usage général et AKS.

S'appuyant sur des décennies d'expérience de Microsoft dans la fourniture de technologies sur site et hybrides aux gouvernements et aux secteurs réglementés, Azure Local fonctionne avec ou sans connectivité cloud, passe de déploiements à nœud unique à ceux atteignant la taille d'un datacenter, et donne aux organisations le contrôle sur l'emplacement de leurs données et sur les personnes pouvant y accéder. Tout en activant la résidence des données, la conformité réglementaire et les performances à faible latence, Azure Local active des capacités innovantes dans des environnements connectés au cloud, connectés par intermittence ou entièrement déconnectés afin de répondre aux exigences de résilience des clients et de continuité d'activité, y compris dans des scénarios très réglementés ou extrêmes.

Environnements connectés

Le cloud privé souverain prend en charge des environnements hybrides qui permettent aux organisations d'étendre les services cloud de Microsoft dans une infrastructure contrôlée par le client, tout en maintenant des capacités de gestion, de sécurité et de conformité cohérentes. Grâce à Azure Local, les clients peuvent gérer des charges de travail dans des environnements locaux et des environnements connectés au cloud grâce à un plan de contrôle unifié, permettant la résidence des données, un traitement à faible latence et une autonomie opérationnelle lorsque cela s'avère nécessaire. Ce modèle hybride est particulièrement adapté aux secteurs réglementés et aux organisations du secteur public qui doivent équilibrer l'innovation et l'extensibilité avec un contrôle local et un alignement réglementaire.

Environnements déconnectés

Pour les scénarios où la connectivité au cloud public est limitée ou non autorisée, le cloud privé souverain prend en charge des opérations entièrement déconnectées. Dans ces environnements, les clients peuvent exécuter des services cloud avec un plan de contrôle entièrement local, ce qui permet aux systèmes de fonctionner de façon sécurisée et indépendante sans dépendre d'un accès réseau externe. Les déploiements déconnectés sont conçus pour prendre en charge des charges de travail critiques, des scénarios en périphérie et des environnements sensibles où les exigences réglementaires, de sécurité ou de résilience nécessitent une isolation, tout en bénéficiant de l'infrastructure, des mises à jour et du cycle de vie validés par Microsoft, ainsi que des processus de gestion.

Feuille de route du cloud privé souverain

Déploiements déconnectés à grande échelle *(en version préliminaire)*

Ces déploiements étendront les points d'échelle de façon à prendre en charge des déploiements Azure Local à grande échelle avec un plan de contrôle déconnecté. Cela signifie que les clients pourront évoluer d'un déploiement à nœud unique ou en cluster vers un environnement déconnecté de racks multiples et de datacenter.

Capacités d'IA souveraines étendues *(en version préliminaire et à venir)*

Ces capacités élargiront la gamme de modèles que les organisations peuvent exécuter localement via Foundry Local et ajouteront des expériences de récupération et agentiques, afin que les équipes puissent créer des applications d'IA fondées sur leurs propres informations entièrement dans l'environnement souverain.

Services de données étendus *(en version préliminaire et à venir)*

Ces services élargiront la gamme de services de données que les organisations peuvent exécuter dans des environnements contrôlés par le client, y compris ceux qui sont entièrement déconnectés. Les charges de travail de données transactionnelles, documentaires et d'application peuvent ainsi accompagner l'IA et les applications qui en dépendent.

Informatique confidentielle étendue pour le cloud privé souverain *(fonctionnalité à venir)*

Cette fonctionnalité étendra la protection matérielle des données en cours d'utilisation aux environnements contrôlés par le client, ce qui permettra aux charges de travail et aux modèles sensibles d'être exécutées avec des protections informatiques confidentielles sur site.

Contrôles des modifications améliorés *(fonctionnalité à venir)*

Ces contrôles introduiront des politiques et processus d'approbation configurables afin de permettre aux organisations de surveiller explicitement les mises à jour et les changements de configuration au fur et à mesure de leur propagation des environnements cloud connectés vers l'infrastructure contrôlée par le client, renforçant ainsi la gouvernance et la conformité.

Récupération d'urgence de site à site *(fonctionnalité à venir)*

Cette fonctionnalité constituera une extension des fonctionnalités de récupération des sites Azure pour Azure Local afin de soutenir la continuité des activités en maintenant la disponibilité des applications et des charges de travail lors de défaillances de l'infrastructure ou de pannes localisées.

De la connexion à la déconnexion totale *(fonctionnalité à venir)*

Cette fonctionnalité continuera de prendre en charge des modèles de déploiement flexibles permettant aux clients de migrer leurs charges de travail des environnements connectés vers des opérations totalement déconnectées, offrant ainsi une autonomie et une résilience plus importantes au fur et à mesure de l'évolution des exigences opérationnelles ou réglementaires.

Écosystème partenaire souverain

Les résultats en matière de souveraineté dépendent non seulement de l'endroit où résident les données et de la manière dont elles sont protégées, mais également de qui conçoit, exploite et régit légalement l'environnement dans lequel elles sont exécutées. L'écosystème partenaire souverain aborde cette dimension. Il étend le Microsoft Sovereign Cloud via des partenaires qui livrent et exploitent des solutions dans leur pays, une spécialisation permettant d'identifier une expertise souveraine validée, un marché de logiciels et services partenaires et, lorsque les exigences nationales l'exigent, des environnements cloud détenus et exploités de manière indépendante par des partenaires nationaux. Ensemble, ces éléments soutiennent le premier des engagements numériques européens de Microsoft, à savoir contribuer à la construction d'un vaste écosystème d'IA et de cloud à travers l'Europe.

Partenaires de souveraineté mondiaux

Les organisations européennes adoptent rarement le cloud souverain de façon isolée. La plupart d'entre elles modernisent des systèmes déjà en production, migrent des charges de travail réglementées et intègrent des exigences nationales en matière d'identité, de sécurité et d'archivage. Ce travail dépend de partenaires ayant une présence locale et une connaissance du secteur.

L'écosystème de partenaires de Microsoft comprend des intégrateurs de systèmes mondiaux, des fournisseurs de services régionaux et nationaux, des éditeurs de logiciels indépendants et des fournisseurs de services gérés, y compris des organisations détenues et gouvernées par le pays. Les clients ont accès à une expertise dans le pays, à une prise en charge de la langue locale et à des arrangements contractuels locaux. La plateforme sous-jacente reste cohérente, tandis que la livraison, les opérations et la responsabilisation sont adaptées aux exigences de chaque juridiction.

Spécialisation en souveraineté numérique

Pour les charges de travail souveraines, la sélection d'un partenaire de livraison est elle-même une décision de contrôle. Pour rendre cette décision vérifiable, Microsoft propose la spécialisation Souveraineté numérique au sein du Microsoft AI Cloud Partner Program.

Les partenaires titulaires de cette spécialisation ont démontré leur expertise dans la prestation de solutions sécurisées, conformes et régies localement sur Azure et Microsoft 365, y compris la résidence des données, les contrôles d'accès opérationnels, le chiffrement et la gestion des clés, ainsi que les cadres réglementaires applicables à des secteurs spécifiques. La spécialisation permet aux clients d'identifier des partenaires qualifiés avant de s'engager. Pour les organismes de réglementation et les fonctions de gestion des risques internes, elle fournit des preuves indépendantes qu'un partenaire a été évalué en fonction d'une norme définie au lieu de se fier à une capacité autodéclarée.

Solutions partenaires sur le marché

Les exigences de souveraineté s'étendent au-delà de la plateforme dans la mesure où elles s'appliquent au logiciel exécuté sur cette dernière. Sur le marché, les clients peuvent identifier des logiciels et services partenaires qui étendent les capacités du cloud souverain dans les domaines de la sécurité, de la conformité, des données, de l'IA, de l'infrastructure et des opérations. Ces solutions sont obtenues par l'intermédiaire de canaux commerciaux établis, ce qui permet aux organisations d'assembler un environnement complet sans opérer en dehors de leur modèle de gouvernance existant.

Clouds partenaires nationaux

En France et en Allemagne, nos clouds partenaires nationaux offrent des instances complètes et indépendantes de Microsoft 365 et Microsoft Azure sous propriété et contrôle nationaux complets.

En France, *Bleu*, une coentreprise entre Orange et Capgemini, exploite un « cloud de confiance » destiné au secteur public français et aux fournisseurs d'infrastructures critiques, conçu pour répondre aux exigences SecNumCloud du gouvernement français (ANSSI).

En Allemagne, *Delos Cloud*, une filiale de SAP, exploite un cloud souverain pour le secteur public allemand, conçu pour répondre aux exigences de plateforme cloud du BSI du gouvernement allemand.

La plupart des organisations utiliseront une combinaison de ces modèles de déploiement, car toutes les charges de travail n'exigent pas le même niveau d'indépendance ou d'isolement. Microsoft Sovereign Cloud permet aux clients de mettre en place les contrôles appropriés dès le départ, afin qu'ils soient prêts à travailler selon les exigences de leur choix à tout moment.

Les opérations de Microsoft en Europe

L’approche de Microsoft en matière de souveraineté en Europe repose sur une gouvernance conforme au droit européen, une responsabilité juridique claire et des contrôles opérationnels transparents. Au lieu de créer une entité juridique isolée pour les charges de travail souveraines, Microsoft propose des résultats en matière de souveraineté grâce à des entités européennes établies, des modèles de gouvernance renforcés et des dispositifs de protection techniques et contractuels exécutoires.

Structure d’entité

Microsoft fournit des services cloud en Europe par l’entremise d’entités juridiques Microsoft établies et exerçant leurs activités dans l’Union européenne (UE), soumises aux lois européennes et alignées sur les exigences réglementaires propres à la région. Ces entités sont responsables de l’exploitation de l’infrastructure et des services cloud européens et concluent des contrats directement avec des clients européens. Nos opérations de datacenters européens sont régies par un conseil d’administration européen qui exerce ses activités conformément à la législation européenne, renforçant ainsi notre engagement envers la surveillance locale. Cette structure assure la continuité de la responsabilité juridique tout en protégeant la cohérence de la plateforme cloud et en offrant un portefeuille de services dans l’ensemble des régions.

Pour les charges de travail nécessitant une indépendance juridique accrue ou un alignement avec des cadres de souveraineté nationale, Microsoft soutient également des clouds partenaires nationaux, tels que ceux situés en France et en Allemagne. Ces environnements sont détenus et exploités de manière indépendante par des entités locales, soumis à la gouvernance d’entreprise locale, à la législation nationale et à la surveillance réglementaire, tout en fournissant la technologie Microsoft conformément à des mesures de contrôle contractuel et opérationnel strictes. Ce modèle permet aux clients de répondre aux exigences nationales sans fragmenter leur architecture cloud plus large.

Gouvernance d’entreprise et contrôles d’accès

Microsoft assure la réalisation des objectifs de souveraineté grâce à un modèle de gouvernance à plusieurs niveaux qui combine des contrôles techniques, une supervision opérationnelle et des engagements légalement contraignants. Cette approche est conçue pour réduire la dépendance envers la fiabilité des opérateurs et donner aux clients un contrôle vérifiable sur l’accès à leurs données.

Au niveau de l’infrastructure, Microsoft protège les données même pendant leur traitement, ce qui permet de s’assurer que les informations sensibles ne pourront pas être accessibles par les opérateurs cloud à moins qu’ils ne possèdent une autorisation explicite. Ces protections sont conçues pour protéger et isoler les données client tout au long de leur cycle de vie, en complétant le chiffrement lorsque les données sont stockées ou transmises, et en réduisant l’exposition à un accès non autorisé, même dans des scénarios opérationnels à privilèges élevés.

Microsoft limite encore l’accès grâce au chiffrement contrôlé par les clients. Avec des options telles que Clés gérées par le client et Gestion externe des clés, les clients conservent l’autorité sur les clés qui protègent leurs données. Sans ces clés, Microsoft ne peut pas lire ou utiliser le contenu du client de façon indépendante, ce qui permet de s’assurer que les décisions d’accès restent sous le contrôle du client.

Lorsqu’un accès opérationnel limité est nécessaire pour maintenir la fiabilité du service, Microsoft applique des contrôles stricts et auditables. La fonction Customer Lockbox nécessite une approbation explicite du client avant que le personnel de Microsoft puisse accéder au contenu client lors d’incidents de support. Pour les opérations européennes souveraines, Data Guardian ajoute une autorisation et une surveillance par du personnel européen, toutes les actions étant consignées dans des journaux infalsifiables. Ensemble, ces mesures peuvent permettre de s’assurer que tout accès privilégié est délibéré, transparent et entièrement traçable.

Engagements juridiques et contractuels pour les demandes d’accès

Microsoft ne donne à aucun gouvernement un accès direct ou sans entrave aux données des clients et gère les demandes d’accès des gouvernements et des forces de l’ordre à l’aide de processus juridiques et opérationnels définis, conçus pour garantir l’alignement sur le droit européen et les intérêts des clients. Pour les services cloud européens, Microsoft opère dans les cadres juridiques européens et toutes les demandes relatives aux données des clients sont examinées individuellement par des équipes juridiques, de confidentialité et de conformité possédant une expertise régionale. Les demandes sont évaluées en fonction de leur territoire, de leur légalité et de leur portée avant toute action, et celles qui ne satisfont pas aux normes juridiques applicables sont contestées ou rejetées.

Conformément à une posture axée sur le client, les conditions contractuelles et les engagements de confidentialité de Microsoft sont conçus pour maximiser le contrôle et la transparence pour les clients. Lorsque cela est légalement autorisé, Microsoft redirige les demandes vers les clients afin qu’ils puissent y répondre directement ou demander un recours judiciaire. Lorsque la notification est autorisée, Microsoft informe rapidement les clients et fournit suffisamment de détails pour permettre une action appropriée. Si la notification est légalement restreinte, Microsoft cherche à lever ou à atténuer ces restrictions. Microsoft s’est également engagée publiquement

à contester en justice les demandes manifestement invalides ou en conflit avec la législation en vigueur, y compris les exigences extraterritoriales non conformes aux normes juridiques européennes, comme le reflètent ses engagements numériques européens et sa promesse de résilience numérique. Microsoft a une longue expérience de contestation réussie d'ordonnances d'interdictions de divulgation, tant directement en communication avec les forces de l'ordre que formellement devant les tribunaux.

Ces engagements juridiques sont renforcés par les contrôles techniques et contractuels décrits ci-dessus, qui limitent l'accès des opérateurs et réduisent l'exposition à la divulgation non autorisée. Ensemble, la responsabilité juridique régionale, les droits exécutoires et les contrôles auditables offrent aux clients l'assurance que les demandes d'accès sont traitées de manière cohérente, transparente et conforme aux exigences juridiques européennes.

Sous-traitants et transparence

Microsoft maintient la transparence concernant l'utilisation des sous-traitants et applique des garanties contractuelles, techniques et organisationnelles conformes aux exigences de protection et de sécurité des données de l'UE. Les sous-traitants font l'objet d'une diligence raisonnable, d'obligations contractuelles et d'une supervision permanente afin de respecter les normes de Microsoft en matière de sécurité, de confidentialité et de conformité.

Des capacités complètes de journalisation et d'audit dans les services cloud de Microsoft permettent aux clients de surveiller les actions administratives, les tentatives d'accès et les opérations sur les données. Les registres d'audit sont protégés contre toute modification non autorisée et soutiennent la gouvernance interne ainsi que l'examen réglementaire externe. Ces mesures techniques sont renforcées par des engagements contractuels exigeant la journalisation, la justification des accès et la notification du client, ce qui permet de s'assurer que la transparence et la responsabilité sont à la fois exécutoires et observables.

Ensemble, la structure organisationnelle de Microsoft, son modèle de gouvernance et ses contrôles des sous-traitants rassurent les clients sur le fait que les services cloud en Europe fonctionnent en respectant une responsabilité juridique claire, une supervision opérationnelle disciplinée et des contrôles d'accès transparents conformes aux attentes en matière de souveraineté européenne.

Concrétiser la souveraineté numérique

Les organisations européennes traversent une période de profonds changements. Les technologies cloud et d'IA redéfinissent la prestation des services publics, la concurrence des industries et le fonctionnement des systèmes critiques, tout cela alors que les attentes réglementaires, les menaces qui pèsent sur la sécurité et l'incertitude géopolitique continuent de s'intensifier. Pour relever ces défis, il ne suffit pas de se conformer aux règles actuelles, il est nécessaire de mettre en place une plateforme cloud conçue pour s'adapter à l'évolution des exigences.

Microsoft Sovereign Cloud a été conçu pour permettre aux organisations de franchir une nouvelle étape en toute confiance. Au lieu d'exiger un cloud distinct ou isolé, Microsoft permet aux clients d'appliquer des contrôles souverains sur l'ensemble de la Microsoft Stack sans sacrifier l'innovation, l'échelle ou les fonctionnalités.

Pour commencer leur parcours de souveraineté numérique dans le cloud public, les organisations peuvent notamment utiliser **la zone d'atterrissage souveraine** (SLZ). Les organisations peuvent commencer par évaluer les exigences de souveraineté par charge de travail et établir une zone d'atterrissage souveraine comme base pour une adoption sécurisée et conforme du cloud et de l'IA. En adoptant la zone d'atterrissage souveraine, les clients peuvent bénéficier d'une architecture pratique qui accélère l'alignement sur les exigences de souveraineté régionale tout en prenant en charge l'évolutivité sur l'ensemble des régions Azure. Au fil du temps, les stratégies et contrôles souverains intégrés continueront de se développer, aidant les organisations à atteindre les résultats souverains prêts à l'emploi plus rapidement et avec une plus grande confiance.

Microsoft a choisi de s'engager sur le long terme. Grâce à des investissements continus, une gouvernance transparente et des garanties juridiquement applicables, notre objectif est d'être un partenaire stable et de confiance pour les gouvernements, les entreprises et les institutions critiques de l'Europe. Microsoft Sovereign Cloud constitue un socle pour l'adoption des technologies cloud et d'IA en toute confiance, tout en favorisant l'innovation, la résilience et le contrôle dans un paysage numérique de plus en plus complexe.

Microsoft

Les informations présentées dans ce document représentent les opinions actuelles de Microsoft Corporation sur les sujets évoqués à la date de cette publication. Étant donné que Microsoft doit répondre aux conditions variables du marché, elles ne doivent pas être interprétées comme un engagement de la part de Microsoft, et Microsoft ne peut garantir l'exactitude de toutes les informations présentées après la date de cette publication.

Ce livre blanc est à caractère informatif uniquement. Microsoft n'accorde aucune garantie expresse ou implicite quant aux informations présentées dans ce document.

Le respect des législations en vigueur en matière de droits d'auteur relève de la responsabilité de l'utilisateur. Sans limiter la portée des droits prévus par le droit d'auteur, aucune partie de ce document ne peut être reproduite, stockée, introduite dans un système d'extraction de données, ni transmise sous quelque forme, à quelque fin ou par quelque moyen que ce soit (électronique, mécanique, par photocopie, enregistrement ou autre) sans l'autorisation expresse et écrite de Microsoft Corporation.

Microsoft est susceptible de détenir des brevets, des dépôts de brevets, des marques déposées, des droits d'auteur ou d'autres droits relatifs à la propriété intellectuelle couvrant des sujets traités dans ce document. Sauf dispositions expresses dans un accord de licence écrit de la part de Microsoft, la fourniture de ce document ne vous accorde aucune licence sur ces brevets, marques déposées, droits d'auteur ou autre propriété intellectuelle.

© 2026 Microsoft Corporation. Tous droits réservés.

Les noms des sociétés et des produits mentionnés dans le présent document peuvent être des marques commerciales de leurs détenteurs respectifs.