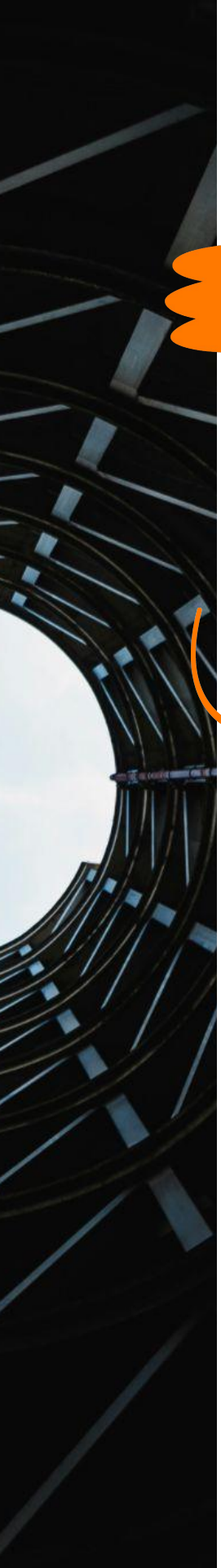
Business

Livre blanc

Cloud de confiance

Réussir sa migration vers Bleu



Sommaire

Cloud de confiance Pourquoi l'inclure dans sa stratégie ?

Si le Cloud public est en plein essor, son utilisation **peut s'avérer risquée, en particulier pour les entités publiques et les entreprises opérant dans des secteurs d'activité sensibles.** En France, c'est le cas des opérateurs d'importance vitale (OIV) et des opérateurs de services essentiels (OSE). Pour cette population disposant de données sensibles, les enjeux de sécurité, de résilience, de confidentialité et d'intégrité sont majeurs, notamment dans un contexte géopolitique tendu et face au durcissement de la réglementation européenne en matière de cybersécurité.

Ainsi, la directive européenne NIS2 (Network and Information Security) va bientôt entrer en application en France. Cette dernière vise à renforcer la résilience et la sécurité des réseaux et des systèmes d'information des opérateurs de services essentiels. De plus en plus d'organisations choisiront un Cloud de confiance pour se conformer à la réglementation, n'ayant pas toujours les ressources nécessaires pour gérer la sécurité en interne.

Avec NIS2, c'est environ **15 000 entités essentielles (EE) ou importantes (EI),** nouvelle dénomination qui remplacera la notion d'OSE, qui sont susceptibles d'être confrontées à ce défi. Et ce, dans de nombreux domaines comme **la banque, la santé, le transport, la gestion de l'eau, l'énergie, l'industrie, l'espace, ainsi que les administrations publiques, et près de 1 500 collectivités territoriales, groupements de collectivités et organismes placés sous leur tutelle.**

< Retour

Cloud de confiance

Emmanuel Cacheux

Chief Trust Officer - Orange Business

« À l'heure où la priorité stratégique de nombreuses entreprises est la protection des données, le Cloud de confiance est la réponse naturelle à ce besoin de sécurité et de souveraineté. Les garanties offertes par cette infrastructure permettent de déléguer le maintien en condition opérationnelle et d'accélérer une transformation numérique essentielle pour concentrer ses efforts sur son cœur d'activité.

La transparence et la résilience du Cloud de confiance permettent de s'assurer que les données les plus sensibles sont strictement utilisées dans un cadre maîtrisé, sans fuites de données.

C'est un élément essentiel de la chaîne de confiance numérique au même titre que la connectivité, une maîtrise de bout en bout de son autonomie stratégique. »

>>

Pour le secteur public, cette évolution réglementaire vient compléter la doctrine "Cloud au centre" de l'État incitant les administrations et les opérateurs étatiques à recourir au Cloud, tout en les sensibilisant à la sécurisation des données susceptibles d'être hébergées et gérées dans le Cloud public. Ensuite, **la loi Sécurité et Régulation de l'Espace Numérique (SREN)**, publiée au Journal officiel le 22 mai 2024, impose au secteur public une meilleure gestion et sécurisation de leurs ressources numériques. Cela s'accompagne d'un renforcement de la souveraineté numérique, à travers notamment la maîtrise des infrastructures critiques, une meilleure protection des données sensibles et le développement de solutions nationales pour limiter la dépendance aux fournisseurs étrangers.

La qualification SecNumCloud 3.2 : le sésame du Cloud de confiance

Pour répondre aux menaces relatives à la sécurité, à la disponibilité, à la gestion des données ainsi qu'à leur confidentialité, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a défini des exigences techniques, opérationnelles et juridiques auxquelles les fournisseurs de services Cloud doivent se conformer pour être qualifiés SecNumCloud.

La qualification SecNumCloud 3.2 est le niveau le plus élevé en matière de sécurité et de gestion des risques. Elle nécessite la conformité à des exigences renforcées de sécurité, la capacité à assurer la résilience et la continuité des services, une gestion avancée des incidents et des vulnérabilités ainsi que la confidentialité, l'intégrité, la disponibilité et la traçabilité des données.

La qualification SecNumCloud 3.2 a vocation à proposer des services hautement sécurisés et héberger des données sensibles.
Cette qualification est aussi et surtout la garantie d'une immunité aux lois non-européenne à portée extra territoriales qui obligent les fournisseurs de services Cloud à transmettre les données de leurs clients à leurs autorités nationales.

À titre d'exemple, le Foreign Intelligence Surveillance Act (FISA) ou encore le Cloud Act permettent aux autorités américaines d'accéder aux données des clients des fournisseurs de services Cloud qui sont établis aux États-Unis, comme AWS, Microsoft ou encore Google. Les données hébergées dans un Cloud de confiance sont donc non seulement sécurisées, confidentielles, mais aussi protégées de ces lois extra territoriales.

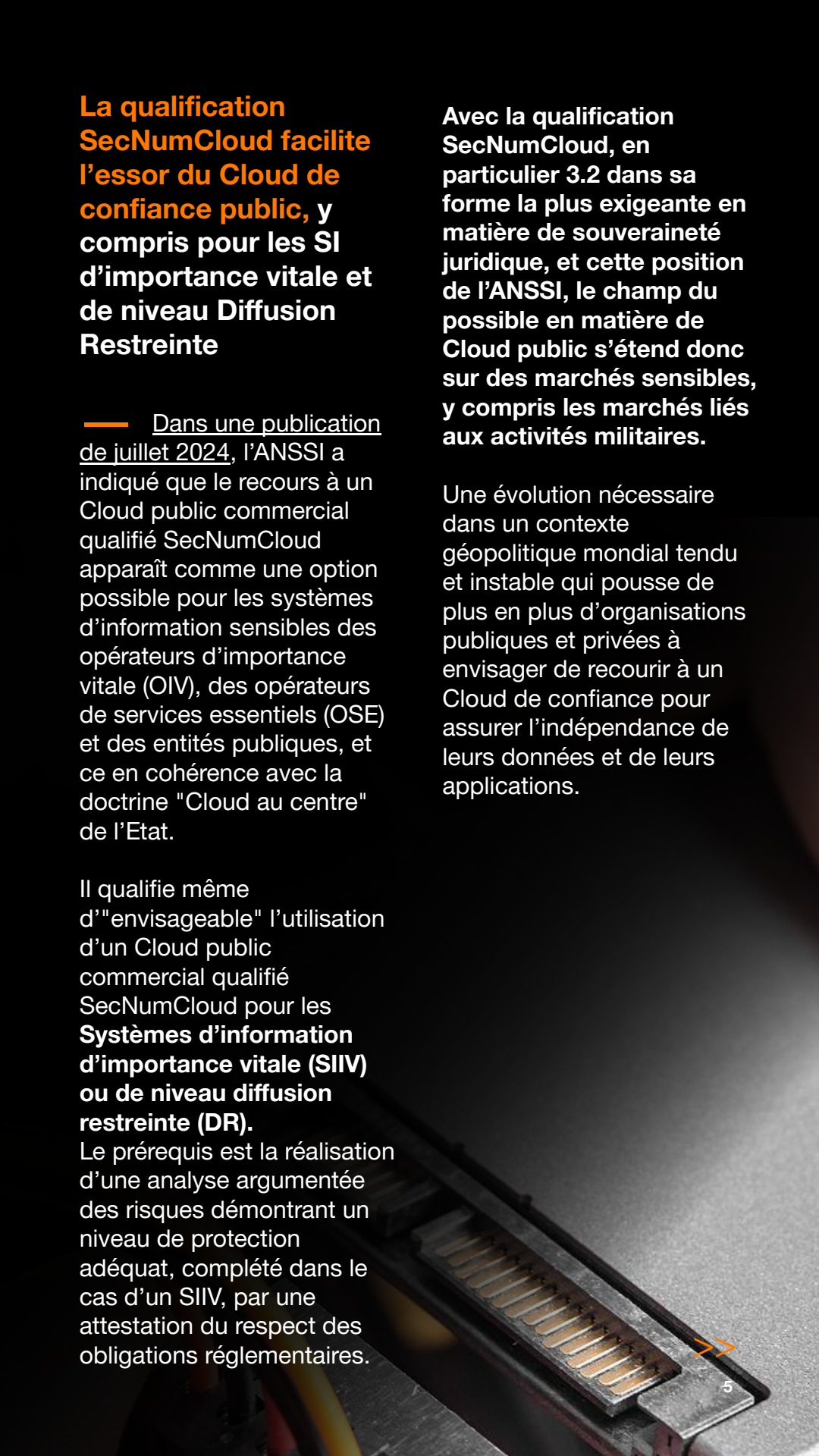
La qualification SecNumCloud facilite l'essor du Cloud de confiance public, y compris pour les SI d'importance vitale et de niveau Diffusion Restreinte

Dans une publication de juillet 2024, l'ANSSI a indiqué que le recours à un Cloud public commercial qualifié SecNumCloud apparaît comme une option possible pour les systèmes d'information sensibles des opérateurs d'importance vitale (OIV), des opérateurs de services essentiels (OSE) et des entités publiques, et ce en cohérence avec la doctrine "Cloud au centre" de l'Etat.

Il qualifie même d'"envisageable" l'utilisation d'un Cloud public commercial qualifié SecNumCloud pour les **Systèmes d'information d'importance vitale (SIIV) ou de niveau diffusion restreinte (DR).**
Le prérequis est la réalisation d'une analyse argumentée des risques démontrant un niveau de protection adéquat, complété dans le cas d'un SIIV, par une attestation du respect des obligations réglementaires.

Avec la qualification SecNumCloud, en particulier 3.2 dans sa forme la plus exigeante en matière de souveraineté juridique, et cette position de l'ANSSI, le champ du possible en matière de Cloud public s'étend donc sur des marchés sensibles, y compris les marchés liés aux activités militaires.

Une évolution nécessaire dans un contexte géopolitique mondial tendu et instable qui pousse de plus en plus d'organisations publiques et privées à envisager de recourir à un Cloud de confiance pour assurer l'indépendance de leurs données et de leurs applications.



Bleu : Cloud de confiance majeur dans le paysage français

Acteur 100% français, Bleu est une joint-venture entre Capgemini et Orange à 50/50, qui a été créée en janvier 2024 et qui dispose de ses propres moyens de fonctionnement. Bleu propose un large catalogue de services de IaaS/PaaS/CaaS et SaaS, en offrant la suite de collaboration et de productivité Microsoft 365, ainsi que les services Microsoft Azure dans un Cloud de confiance. Bleu opère ses services sur le territoire national et dispose de ses propres centres de données situés en France sur deux régions complètement distinctes et étanches des régions Azure de Microsoft, et contractualise avec ses clients en droit français.

Bleu cible les entités publiques et les entreprises opérant sur des secteurs d'activité sensibles, à savoir les opérateurs d'importance vitale (OIV) et les opérateurs de services essentiels (OSE).

L'infrastructure résiliente de Bleu, indépendante de celle de Microsoft, se compose actuellement de deux datacenters (1+1) situés en France (3+1 ultérieurement), chacun d'eux étant connecté en haute redondance avec 3 liens fibrés sur des chemins distincts restant sur le territoire national. Les centres de données sont conçus pour assurer une haute disponibilité des données et une continuité de service.

Les opérations sont gérées en 24x7 de façon autonome par les équipes de Bleu, sous contrat de droit français, réparties dans deux centres opérationnels situés en Ile-de-France et en région Rennaise. Elles assurent la sécurité et la maintenance matérielle des datacenters, l'exploitation et la cybersécurité des services (un SOC en propre), la gestion des réseaux et le support aux clients.

Avec des données hébergées en France, et une qualification SecNumCloud 3.2 en cours auprès de l'ANSSI, **Bleu garantit une immunité aux lois non-européenne à portée extraterritoriale,** comme le Cloud Act, le Foreign Intelligence Surveillance Act ou encore le Patriot Act qui imposent aux fournisseurs de services Cloud établis aux États-Unis d'autoriser l'accès aux données de leurs clients par les autorités américaines.

Laurent Lemaire
Directeur Commercial, Marketing et Partenariats de Bleu

« Créer un environnement numérique sécurisé et responsable pour permettre aux acteurs français de libérer leur potentiel en toute confiance, c'est l'ambition qui guide Bleu depuis sa création. Dans cette dynamique, Orange Business s'est imposé naturellement comme un partenaire stratégique, engagé dès l'origine. Son expertise des environnements critiques, sa maîtrise des technologies Microsoft et sa capacité à accompagner les clients de bout en bout font de lui un acteur de choix pour accompagner les organisations sensibles vers le Cloud de Bleu.

www.bleucloud.fr

Les services Azure et Microsoft 365 dans le Cloud de Bleu

Bleu a pour objectif de proposer l'ensemble des services Azure et Microsoft 365 dans un environnement de confiance et ce, avec les mêmes SLAs. Une offre « renforcée » par rapport à celle de Microsoft dans le Cloud public, notamment en matière d'immunité aux lois extraterritoriales, de réglementation, de localisation ainsi que d'intégrité et de confidentialité des données.

Pour faciliter la migration vers ses services, Bleu a mis en place avec ses partenaires le programme « Départ Lancé ». Une approche en trois étapes (anticiper, préparer, adopter) comportant une quarantaine d'actions techniques et organisationnelles.

Orange Business a été le premier partenaire à être qualifié « Départ Lancé » par Bleu. Un partenariat enclenché très tôt qui a permis à Orange Business d'accompagner dès 2024, un premier client dans la préparation à sa migration vers le Cloud de Bleu.

Géraldine Steinberg

Chief Partner Officer,
Orange Business

« Le Cloud de confiance est au cœur de la stratégie Cloud d'Orange Business. C'est un enjeu désormais central pour nos clients en France et Orange Business dispose d'atouts uniques comme son expertise, son engagement et son rôle d'opérateur de confiance. Il était donc naturel que Bleu et Orange Business s'associent dès mars 2024. Ainsi, Bleu a rejoint le cercle de la vingtaine de partenaires stratégiques pilotés au plus haut niveau de notre organisation. »

>>

Les facteurs clés pour réussir sa migration vers Bleu

Un projet de migration vers un Cloud de confiance comme Bleu, c'est un ensemble de compétences à mobiliser de la phase d'étude jusqu'au déploiement, incluant notamment la cybersécurité, la maîtrise des réglementations, une expérience des projets de migration vers le Cloud, un niveau de connaissance poussé des technologies Microsoft, la capacité à prendre en compte l'impact organisationnel au niveau de la DSI et l'accompagnement au changement des utilisateurs, sans oublier une forte expertise en matière de connectivité réseau.

Le DSI a le choix entre sélectionner un partenaire multi-spécialiste ayant l'expérience et les compétences pour maîtriser l'ensemble de ces sujets ou recourir à plusieurs partenaires, ce qui peut contribuer à complexifier la conduite du projet et peser sur son bon déroulement.

Orange Business est en mesure de répondre à cette problématique et de proposer un accompagnement de bout en bout à ses clients grâce au large éventail de compétences dont il dispose en matière de conseil dans les projets de transformation digitale, d'audit, de cybersécurité, de déploiement de solutions Microsoft (avec plus de 2 300 clients accompagnés et 2 400 certifications) mais aussi de connectivité réseau à Bleu, de solutions d'hybridation ou encore de services managés (FinOps, Devops, services de sécurité…), une fois la migration réalisée.

Nos échanges avec les DSI montrent à quel point cette expertise est essentielle pour les aider à élaborer leur stratégie de migration vers un Cloud de confiance et à en maîtriser le déploiement.

Les entreprises opérant dans des secteurs d'activité très sensibles et qui souhaitent migrer tout ou partie de leur **système d'information d'importance vitale (SSIV) ou de type diffusion restreinte (DR)** dans un Cloud de confiance, doivent se conformer à une homologation permettant à l'ANSSI de s'assurer qu'ils n'existent pas de risques significatifs. À ce titre, **Orange Business et Orange Cyberdefense ont été référencés par Bleu pour réaliser l'homologation SIIV et DR.**

Les étapes clés d'une migration vers un Cloud de confiance

Pour réussir sa migration vers Bleu, une préparation rigoureuse est essentielle. Il s'agit d'analyser l'existant, de cartographier les données sensibles et les applications à migrer. Pour Microsoft 365 et les applications collaboratives, il faut aussi identifier les utilisateurs concernés et leurs usages. Ce cadrage influence les choix d'hybridation et la gestion des tenants, un aspect souvent sous-estimé.

Il convient également de compléter l'expression du besoin par la prise en compte **des aspects organisationnels de la DSI** pour voir dans quelle mesure elle dispose des compétences et d'une gouvernance qui lui permettra de conduire sa stratégie de migration.

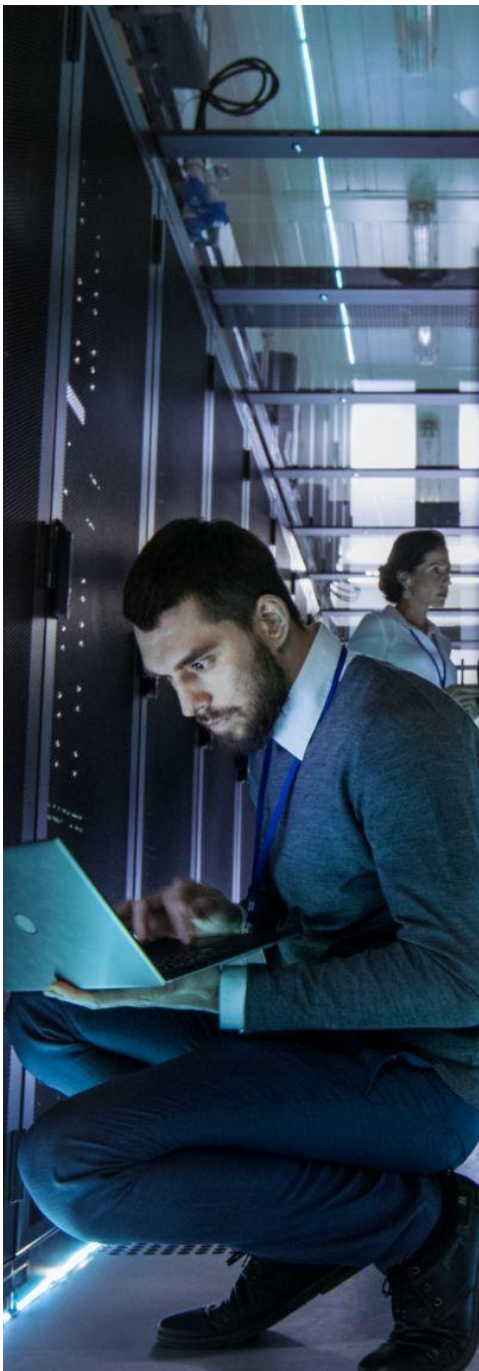
Ce sera aussi une façon d'arbitrer entre plusieurs scénarios d'utilisation qui peuvent être envisagés en fonction de leur impact plus ou moins élevé sur l'organisation et les risques qui en découlent. Cet arbitrage peut aussi être complété par une analyse technico-économique.

Dans le cadre d'une migration vers Microsoft 365 dans Bleu et ses de solutions de communication et collaboratives, **les entreprises sont souvent demandeuses d'un accompagnement pour élaborer un plan facilitant l'adoption et la formation des utilisateurs.** Une demande à laquelle Orange Business sait répondre. La prise en compte de la dimension humaine se révèle particulièrement importante, notamment quand l'entreprise n'utilise pas encore les produits Microsoft ou les utilisent en version on-premise, avec des fonctionnalités qui peuvent différer par rapport au Cloud.

Une fois les besoins et l'architecture cible définis, les éventuels plans d'adoption et de formation anticipés, l'élaboration de la feuille de route est une étape clé pour laquelle un accompagnement de la DSI se révèle pertinent pour bien identifier les chantiers à mener, les prioriser dans le temps et définir les moyens nécessaires à leur réalisation.

Enfin, lors du déploiement, **il faut prévoir un travail significatif de paramétrage des services et de sécurisation des identités,** en particulier en cas d'hybridation, y compris entre Bleu et le Cloud public de Microsoft, le multi-tenant entraînant une segmentation de l'administration des ressources et des configurations. C'est un élément qui doit être anticipé lors de l'analyse de l'existant et l'expression du besoin, comme évoqué précédemment.

À titre d'information, il existe plus de 200 recommandations de sécurité sur un tenant Microsoft 365 qui nécessitent d'intervenir sur plus d'un millier de paramètres.



Paroles d’experts

Bien préparer sa migration

Fort de son expertise dans le domaine des études stratégiques pour le secteur privé, public et de la défense, notamment dans la transformation digitale et l’adoption du Cloud, **Orange Consulting se positionne comme un partenaire privilégié pour aller vers le Cloud de confiance.**

Orange Consulting accompagne efficacement les organisations privées et publiques dans la préparation de leur migration vers un Cloud sécurisé. Son approche repose sur l’échange et la co-construction, garantissant ainsi une transition fluide et adaptée aux besoins spécifiques de chaque client. En effet, pour Thierry Gluzman, Senior Manager CIO Advisory, l’adoption des nouvelles pratiques autour de zones de données et d’applications dans un espace de confiance, s’accompagne d’un travail sur mesure pour transformer la gouvernance, mais également plus finement les processus. Une mutation réussie s’affirme donc aussi pleinement par une étude détaillée d’évolution du modèle opérationnel IT.

Thierry Gluzman
Senior Manager CIO Advisory

« L'adoption des nouvelles pratiques autour de zones de données et d'applications dans un espace de confiance, s'accompagne d'un travail sur mesure pour transformer la gouvernance, mais également plus finement les processus. »

Thierry Hamelin, Senior Manager en Conseil Move to Bleu, ajoute que la capacité d'Orange Consulting à intervenir à fois sur les volets techniques et organisationnels des transformations, est un atout. Accompagner les organisations lors des grandes étapes préparatoires de leur projet, à savoir l'analyse de l'existant, la définition de la cible, l'élaboration de leur feuille de route est un facteur de succès majeur pour tout projet de migration vers un Cloud. En ce sens, Orange Consulting s'inscrit rigoureusement dans la démarche « Départ lancé » de Bleu sur les phases « Anticiper » et « Préparer ».

Amina Bensetti, Manager IT & Réseau, pilote une mission de migration de Skype vers Teams dans Bleu pour un grand groupe bancaire français et ses 80 000 utilisateurs. Selon elle, la force d'Orange Consulting réside à la fois dans son expertise pointue et dans sa capacité à piloter des projets complexes de bout en bout. La mission qu'elle mène s'inscrit dans une approche adaptative, alignée sur les priorités du client, et par la mobilisation des expertises nécessaires pour accompagner la transformation sur l'ensemble des volets techniques.

Amina Bensetti
Manager IT & Réseau

« Notre agilité a permis d'intervenir efficacement sur des sujets variés tels que l'hybridation, l'observabilité, la connectivité ou encore l'authentification pour accompagner la transformation vers Bleu d'un grand groupe bancaire français sur l'ensemble des volets techniques »

Cette agilité a permis d'intervenir efficacement sur des sujets variés tels que l'hybridation Skype/Teams, l'observabilité, la connectivité ou encore l'authentification. C'est un exemple concret de notre approche sur mesure de co-construction, basée sur des ateliers de travail avec les équipes du client. Un travail essentiel permettant de cadrer les différents scénarios de migration, de structurer les projets à engager et de poser les étapes intermédiaires vers la cible.

De leurs côtés, Pierrick Besson, Directeur Conseil Modern Workplace et Jean-Michel Menant, Directeur Expérience Employés chez Orange Consulting, soulignent la valeur ajoutée d'une approche par métier / personae pour garantir une expérience utilisateur efficace et adaptée sur Bleu. Il est important d'identifier par cible les usages pour structurer la feuille de route de migration, ainsi que ses impacts en termes techniques et d'accompagnement des utilisateurs.

>>

Cette réflexion permet aussi de définir une gouvernance des usages pour les environnements hybrides Microsoft 365 et Bleu.

En résumé, pour Guillaume Grard, Directeur d'Orange Consulting, migrer une partie de son patrimoine vers un Cloud de confiance est un projet à part entière. Et ce n'est pas qu'un projet Cloud et technologique. Il doit être anticipé et soigneusement préparé. La notion de confiance ne s'arrête pas au Cloud. Il faut envisager les aspects de connectivité sécurisée et souveraine, adapter l'écosystème en passant par les processus de développement.

Êtes-vous souverain si vos développeurs sont en off-shore ? Êtes-vous souverain si vous consommez vos applications via des flux Internet non sécurisés ? Êtes-vous souverain si vous ne maîtrisez pas qui utilisent vos applications ?

Orange Consulting, avec la force des groupes Orange Business et Orange Cyberdefense, peut vous accompagner de bout en bout sur les aspects Cloud, Réseau, Cybersécurité, Opérations et transformation des usages car nous sommes le seul intégrateur opérateur partenaire de Bleu.

Le rôle clé de la cybersécurité

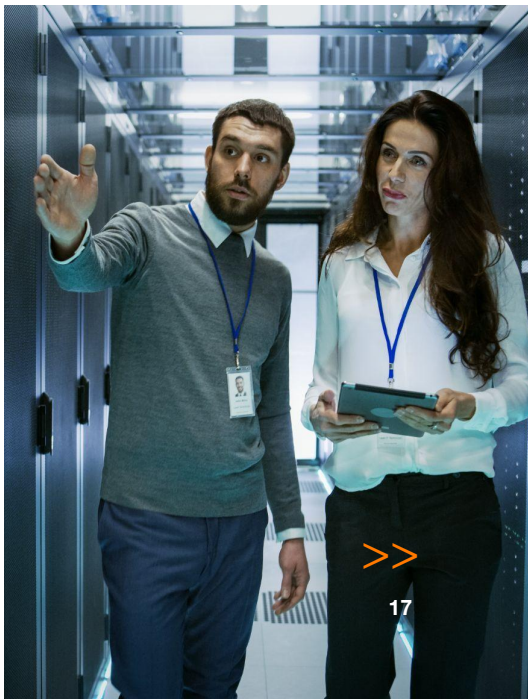
Orange Cyberdefense est l'entité experte en cybersécurité du groupe Orange, proposant des solutions innovantes pour protéger les entreprises et organisations des menaces numériques. Elle offre des services de détection, de réponse et de gestion des incidents, ainsi que des prestations d'audit et conseil en sécurité. Son expertise repose sur une infrastructure mondiale et une équipe d'experts dédiée.

Sébastien De Lattin, Responsable de la Business Unit Microsoft Security, et Axel Beiner, Responsable Sécurité du Cloud au sein de la Business Unit Conseil & Audit, partagent leurs visions et retours d'expériences concernant les enjeux stratégiques, techniques et organisationnels d'une migration vers un Cloud de confiance.

La préparation : un enjeu clé

Une migration réussie nécessite une préparation rigoureuse. Sébastien souligne l'importance de cartographier et classifier les données sensibles avant toute migration et de valider les prérequis techniques et organisationnels. Axel ajoute : « il faut identifier les actifs critiques, évaluer la maturité Cloud du client et concevoir une architecture cible adaptée, en tenant compte des services qualifiés SecNumCloud ».

Nos experts recommandent par ailleurs d'anticiper les enjeux spécifiques, en utilisant notamment des solutions de chiffrement robustes et en déployant des politiques de sécurité renforcées.



Les défis spécifiques d'une migration vers Bleu

Sébastien met en avant les contraintes liées à la gestion des identités et à l'authentification : « passer à une authentification moderne avec MFA peut être un défi pour les entreprises habituées à des protocoles legacy ». Sur le plan organisationnel, Axel note que la coordination entre les équipes Cloud, sécurité et métiers est cruciale, mais souvent complexe. La mise en place d'une matrice RACI claire est donc indispensable pour éviter les blocages.

La sécurité, une priorité absolue

La sécurité est au cœur des préoccupations des clients migrants vers un Cloud de confiance. Sébastien rappelle donc l'importance de déployer des stratégies de DLP (Data Loss Prevention), de classifier les données et d'utiliser des solutions de chiffrement avancées comme le HSM. Axel ajoute que le référentiel SecNumCloud est la base pour garantir une sécurité et une conformité optimale. Nos experts soulignent également l'importance de la surveillance continue. « La mise en place d'outils de monitoring pour détecter les dérives et garantir une non-régression est essentielle » précise Sébastien.

< Retour

Sébastien De Lattin

Responsable de la Business Unit Microsoft Security.

« Passer à une authentification moderne avec MFA peut être un défi pour les entreprises habituées à des protocoles legacy »

>>

L’accompagnement des clients est un pilier central pour assurer la réussite des projets de migration. Axel explique : « nous aidons les clients à concevoir des architectures sécurisées dès le départ pour éviter des ajustements coûteux par la suite ». Sébastien complète : « nous proposons des outils de posture de sécurité pour permettre aux clients de suivre en temps réel leur niveau de sécurité et d’identifier les points à améliorer ». Nos experts insistent aussi sur la formation et la sensibilisation des équipes internes des clients pour garantir une adoption fluide des nouvelles pratiques.

Le Cloud de confiance Bleu : une solution d'avenir

Le Cloud de confiance Bleu se positionne comme une solution incontournable pour les entreprises ayant des besoins de conformité réglementaire. Axel estime ainsi que le référentiel SecNumCloud deviendra la norme de référence pour les projets Cloud de confiance. Sébastien conclut : « le Cloud de confiance répond à une demande croissante de contrôle et de transparence sur les données. Avec l'évolution des réglementations, de plus en plus d'entreprises, même hors OIV, pourraient être amenées à adopter Bleu ».

Orange Cyberdefense est fier d'accompagner les organisations publiques et les entreprises souhaitant héberger des SI sensibles ou Diffusion Restreinte (II901 et SIIV) dans leur transition vers le Cloud Bleu. Notre approche intégrée, nos qualifications ANSSI PRIS, PDIS, PASSI et PACS, garantissent la sécurité des environnements numériques, assurant un continuum sécurisé pour les données et les utilisateurs jusqu'au Cloud Bleu.

Les témoignages de Sébastien et Axel démontrent les enjeux stratégiques, techniques et organisationnels liés à la migration vers un Cloud de confiance. Avec Bleu, Orange Cyberdefense se positionne comme un partenaire de confiance pour accompagner les entreprises dans cette transition cruciale, en garantissant sécurité, conformité et souveraineté des données.

>>

< Retour

Axel Beiner
Responsable Sécurité du Cloud au sein de la Business Unit Conseil & Audit

« Nous aidons les clients à concevoir des architectures sécurisées dès le départ pour éviter des ajustements coûteux par la suite »

Infrastructure et applications : les enjeux techniques et organisationnels d'une migration vers un Cloud public sécurisé

Parmi nos experts au sein de l'entité Digital Services d'Orange Business, Alexandre Saker, Matthieu Petite et Jonathan Jehanno occupent des rôles de Senior Architect spécialisés dans les projets de migration Move-to-Cloud sur Microsoft Azure et Bleu. Ils partagent leur vision et leurs expériences sur les enjeux techniques et organisationnels liés aux projets de migration vers un Cloud public sécurisé, apportant ainsi une valeur ajoutée essentielle pour réussir ces transitions stratégiques.

Synergie entre stratégie financière et technique : gestion d'un déploiement critique

La DSI d'un grand groupe a décidé de migrer son SI sur la technologie Azure dans les Clouds publics de Microsoft et de Bleu, suite à une décision de décommissionner ses data centers historiques, conformément à la nouvelle stratégie groupe. Sous la pression du timing, la DSI a été contrainte de lancer des phases préliminaires de Build au fur et à mesure de la finalisation du design global, au risque de précipiter un déploiement et de provoquer ultérieurement des impacts financiers et organisationnels.

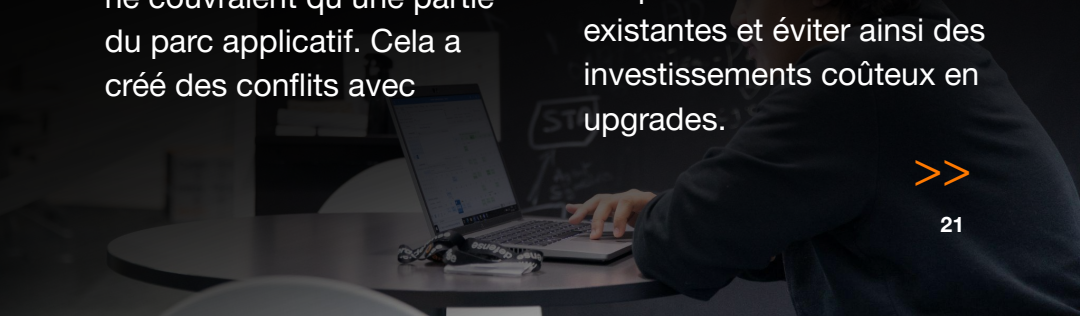
Afin d'éviter les risques de désalignement entre un déploiement contraint dans le temps et le design d'une cible stratégique à long terme une approche intégrée a été proposé par nos experts. En tenant compte de paramètres clés tels que la réglementation (LPM, NIS2, PCI-DSS) et la priorisation du parc applicatif selon sa valeur business, un design de bout en bout a été accéléré pour rester compatible avec les délais du plan financier.

Ce travail a permis de fournir à la DSI des éléments factuels et chiffrés pour contrôler son plan d'exécution, évitant ainsi les pièges potentiels d'une mise en œuvre précipitée. La démarche a assuré une transition maîtrisée, alignant la stratégie financière avec les impératifs techniques et réglementaires, tout en garantissant la continuité des activités.

Migration cloud : continuité, gestion des risques et optimisation

Notre client, en pleine transition vers un Cloud public de confiance, doit gérer des opérations critiques, des environnements obsolètes et des défis organisationnels.

Lors d'une phase pilote de migration en autonomie vers le Cloud public, le client a rencontré des problèmes liés à l'hétérogénéité des technologies de déploiement automatique, notamment l'infrastructure-as-code, qui ne couvraient qu'une partie du parc applicatif. Cela a créé des conflits avec les procédures manuelles, entraînant des dérives de configuration (configuration drift) et des écarts avec les modèles opérationnels. Pour y remédier, nous avons harmonisé les méthodes de déploiement et intégré une gestion approfondie des processus métier, afin de préparer les phases ultérieures. Ainsi, la phase suivante concerne la migration urgente des applications historiques hébergées sur une plateforme on-premise obsolète, souffrant d'une dette technique importante, avec des licences non renouvelées et un support abandonné par l'éditeur. De plus, la saturation du réseau compliquait la migration, provoquant retards et dégradation des performances. Notre équipe a optimisé le réseau existant en déployant des ajustements spécifiques, suspendu temporairement l'utilisation de Shadow IT (non essentielle) pour libérer des capacités en utilisant uniquement les ressources existantes et éviter ainsi des investissements coûteux en upgrades.



Une autre phase a pour but de migrer une application Big Data critique manipulant plusieurs téraoctets de données en ligne, et cela sans aucune interruption de service.

Nous avons conçu une solution en double run, permettant de faire fonctionner simultanément l'environnement existant et la nouvelle infrastructure. En résumé, cette démarche intégrée garantit une migration sécurisée, fluide et maîtrisée, en assurant la continuité des services, en gérant efficacement les déviations et risques, et en optimisant les ressources existantes dans un contexte d'obsolescence et de saturation.

Alexandre Saker
Senior Architect Microsoft Azure & Bleu

« Certaines DSI ayant les compétences pour gérer la complexité d'un Move-to-Cloud lancent leur migration en toute autonomie. Cependant, elles font souvent appel à nous lorsque des difficultés imprévues surgissent, généralement dues à l'absence d'un design global de la cible à long terme. Ce design doit prendre en compte un ensemble complexe de contraintes de l'existant, les impératifs de continuité de service, ainsi que l'adaptation organisationnelle nécessaire. »

Accompagnement global Move-to-Cloud : culture, compétences et autonomie

Pour réussir une migration vers Bleu, il est essentiel d'accompagner l'organisation à la fois sur le plan culturel et opérationnel. Notre approche repose sur deux axes complémentaires : l'acculturation et le transfert de savoir-faire.

Lors de la conception des architectures et des fondations pour la migration, une étape d'acculturation est intégrée pour sensibiliser et former les équipes internes aux principes, aux bonnes pratiques et au mode de fonctionnement du Cloud public. Cette phase vise à favoriser une adaptation efficace, à encourager l'appropriation par les collaborateurs impactés, et à réduire les résistances au changement. En intégrant cette dimension culturelle, nous facilitons l'intégration des nouvelles méthodes, garantissant ainsi une transition durable et réussie.

Parallèlement, un processus d'onboarding est déployé pour transformer les équipes internes, souvent composées de profils SysOps, en une équipe de Cloudops autonome. À travers des ateliers de peer-programming et des sessions de formation pratique, nous transférons progressivement nos compétences en tant…

Matthieu Petite
Senior Architect Microsoft Azure & Bleu

« Au-delà des défis techniques, la réussite d'une migration vers Bleu repose avant tout sur notre capacité à accompagner l'adaptation des compétences, des processus et des outils de notre client à la nouvelle solution. »

>>

qu'intégrateur spécialisé. Cette démarche garantit leur autonomie à long terme, en leur permettant d'adopter de nouvelles pratiques telles que la supervision, le DevOps ou encore la FinOps, dans une organisation plus agile et adaptée aux environnements Cloud de confiance.

Jonathan Jehanno
Senior Architect Microsoft Azure & Bleu

« Lors d'une migration Move-to-Cloud, il peut s'avérer que des impératifs, qu'ils soient réglementaires ou pas, empêchent la migration complète des données vers un Cloud public. Dans ces situations, nous déployons des solutions adaptées telles que l'hybridation avec du Cloud Privé ou du Edge Cloud. L'accompagnement par un partenaire multi-spécialiste, maîtrisant la complexité et la diversité des technologies Cloud, demeure la meilleure garantie pour réussir sa migration en toute confiance. »

Solution d'hybridation sur mesure pour un client multi-sectoriel

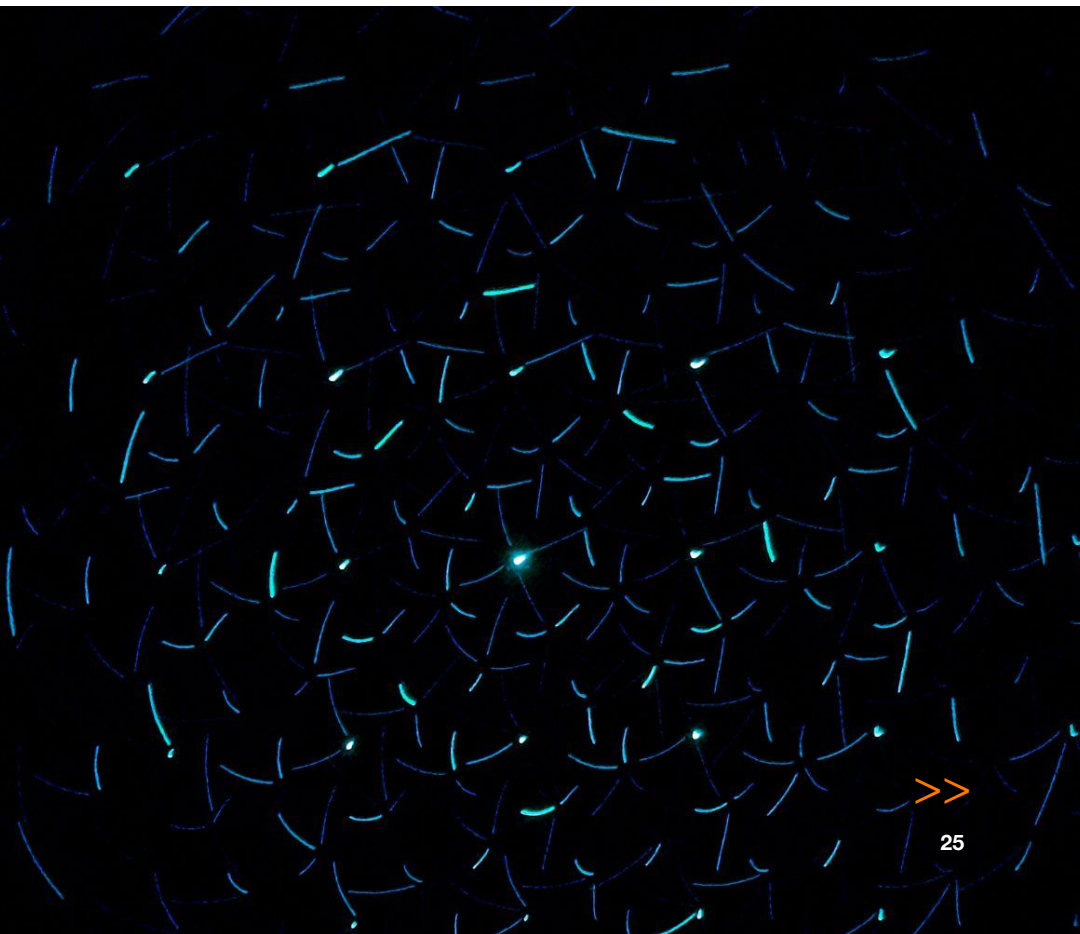
Un client opérant dans les secteurs de la gestion de centres d'appels régionaux et le trading, doit faire face à des contraintes réglementaires strictes, tout en recherchant flexibilité, performance et sécurité.
En effet, le client souhaite migrer progressivement l'essentiel de son système d'information, ancien de dix ans, vers un Cloud public de confiance pour bénéficier de l'évolutivité, de la flexibilité et des coûts maîtrisés du Cloud, tout en respectant strictement les contraintes réglementaires.

Cependant, les données liées aux centres d'appels, doivent impérativement rester hébergées sur site pour respecter la conservation réglementaire.

De plus, les fichiers sensibles liés au trading doivent aussi rester sur des infrastructures privées et nécessitent un accès rapide, sécurisé, et une disponibilité dans plusieurs régions géographiques, avec des délais de transfert de gros fichiers inférieurs à une minute.

Nos experts ont mis en place une architecture hybride sur mesure intégrant du stockage local sécurisé pour les données sensibles, garantissant leur conformité réglementaire et leur confidentialité ainsi que du Edge Computing pour garantir les transferts rapides de gros fichiers de Trading entre plusieurs régions.

Cette solution d'hybridation sur mesure qui combine Cloud public et Cloud privé permet à notre client de concilier conformité réglementaire, sécurité, performance et évolutivité, en s'appuyant sur une architecture flexible et adaptée à ses besoins multi-sectoriels.



Les spécificités des applications de productivité

Grâce à son expertise dans les migrations de messageries et d'environnements collaboratifs, l'entité UNITI d'Orange Business accompagne les organisations dans leur transition vers le Cloud. **Avec son expertise des technologies Microsoft et sa forte sensibilité à la confiance numérique, UNITI offre un accompagnement complet de migration vers le Cloud de confiance Bleu**, de l'évaluation initiale à la mise en œuvre opérationnelle, en passant par la définition de stratégies adaptées aux enjeux de chaque client.

Migrer en toute confiance : les étapes clefs

La réalisation d'une migration implique une série d'étapes techniques essentielles pour garantir la réussite et la sécurité du projet. Selon Pierre-Emmanuel Duc, Business Developer et Expert Microsoft et Bleu, il est crucial d'identifier, classifier et organiser les données à migrer, en distinguant celles qui sont sensibles, critiques ou peu utilisées.

Cette segmentation permet d'établir un plan de migration adapté, avec des phases de transfert progressives et contrôlées. La gestion des accès et des identités doit également être ajustée, notamment par la synchronisation des identités via Entra ID, afin d'assurer une expérience utilisateur fluide. La mise en place d'authentification multifacteur, et de politiques d'accès granulaires est essentielle pour garantir la sécurité, tout en facilitant l'accès aux ressources.

La gouvernance des fédérations d'identités - qu'elles soient ouvertes, fermées ou hybrides - constitue par exemple un paramétrage clef. Celle-ci doit être définie en fonction des enjeux de sécurité, de conformité et de gestion des accès, afin d'assurer une intégration cohérente et sécurisée des différents environnements.

La planification et l'orchestration de la migration doivent être réalisées avec précision, en planifiant chaque étape pour minimiser l'impact sur la production. Cela inclut la sécurisation des flux de données (mise en place de VPN et de firewalls avancés par exemple), la configuration des services, et la validation à chaque étape pour assurer la conformité et la performance. La gestion des flux de messagerie, la sécurisation des échanges, et la conformité réglementaire doivent être intégrées dès la conception. Enfin, chaque étape doit faire l'objet de tests rigoureux pour valider la conformité, la performance et la sécurité, avec des plans de retour arrière en place pour pallier tout incident ou imprévu.

L'hybridation : faire cohabiter plusieurs environnements sans compromis

Comme le souligne Eliott Vernières, Ingénieur Avant-Vente et Expert Microsoft et Bleu, l'un des premiers défis techniques consiste souvent à définir une architecture Cloud robuste, capable de supporter la complexité des environnements. Aujourd'hui, de nombreux clients migrent vers l'offre Cloud public de Microsoft, et cette tendance devrait perdurer : ces environnements ne seront pas ou peu délaissés. La majorité de ces clients adoptera donc une démarche d'hybridation où on-premise, Cloud privé et Cloud public cohabiteront pour répondre à leurs besoins métier, réglementaires ou de sécurité. C'est dans ce contexte qu'Orange Business intervient : accompagner chaque client dans le choix stratégique de la solution la plus adaptée à ses besoins, qu'il s'agisse d'une migration complète ou d'une architecture hybride.

Eliott Vernières
Ingénieur Avant-Vente et Expert Microsoft et Bleu

« L'hybridation des environnements Cloud et on-premise nécessite une orchestration précise, où chaque composant doit être intégré dans une stratégie globale de gouvernance, pour garantir la sécurité et la continuité des services. »

>>

Avec l'un de nos clients, un acteur important du secteur bancaire, nous travaillons par exemple à l'évolution de son système d'information vers une architecture hybride intégrant à la fois Bleu, le Cloud public Microsoft mais aussi son infrastructure existante on-premise. Il ne s'agit pas simplement d'accompagner une migration Skype on-premise vers Teams dans Bleu, mais d'orchestrer une évolution bien plus complexe, impliquant une transformation en profondeur. Pour faire fonctionner ces environnements en harmonie, sans perturber la productivité ni compromettre la sécurité, nous collaborons sur une analyse fine des besoins et des usages de notre client, afin de déterminer quoi, quand, où et comment migrer, pour bâtir une solution sécurisée et adaptée. Force de proposition, le client nous avait confié lors de cette démarche qu'il rencontrait des difficultés à garantir la protection de ses données sur son infrastructure existante, ce qui montre l'importance d'accorder une attention particulière à la sécurisation de ses données.

Nous travaillons également sur la synchronisation efficace de ses annuaires Active Directory, de ses flux réseau, de ses services Exchange, et d'autres composants critiques. La gestion de ces éléments doit être transparente pour les administrateurs et les utilisateurs finaux, tout en garantissant la sécurité et la conformité réglementaire. Encore une fois, la gestion des flux de données, la sécurisation des échanges et la maîtrise des noms de domaine sont autant de défis techniques que nous maîtrisons pour déployer ces solutions en toute sécurité.

Une gouvernance solide : le facteur de réussite

La réussite d'une migration repose enfin sur une gouvernance solide. Pierre-Emmanuel Duc et Eliott Vernières mettent tous deux en avant l'approche d'accompagnement proposée par Orange Business, qui couvre tous les aspects du projet : stratégique, organisationnel et technique. Cela inclut une analyse approfondie des besoins, l'évaluation des infrastructures existantes, la co-construction d'une stratégie de migration sur mesure, ainsi que la mise en place d'une gouvernance projet adaptée pour piloter efficacement le changement.

La maîtrise des environnements Microsoft 365, combinée à une forte sensibilité à la confiance numérique et à la souveraineté, permet à UNITI et à Orange Business de s'adapter aux spécificités de chaque client, garantissant ainsi une migration vers Bleu fluide, sécurisée et alignée avec les enjeux métiers.

Pierre-Emmanuel Duc
Business Developer et Expert Microsoft et Bleu

« Réussir une migration vers le Cloud Bleu, c'est avant tout instaurer une gouvernance robuste qui sert de socle à l'ensemble du projet. En structurant la gestion des identités, des accès et des données, on crée un environnement sécurisé où chaque acteur peut évoluer en toute confiance. »

< Retour OK >>

La connectivité : un élément à ne pas négliger

Mettre ses données dans un environnement situé en France, sécurisé avec les plus fortes exigences de l'ANSSI (cloisonnement, cryptographie, monitoring…), opéré dans les limites du territoire européen, et étanche aux lois extra territoriales américaines permet de protéger les données les plus sensibles.

Mais il ne faut pas sous-estimer l'enjeu que représente l'accès aux infrastructures sécurisées. L'accès aux offres Cloud se fait majoritairement depuis le réseau Internet public, de manière sécurisée (avec chiffrement) ou non. Cette connectivité a ses limites que ce soit en termes d'intégrité, de confidentialité (même en cas de chiffrement) ou encore de latence.

Antoine Soubigou
Architecte Cloud Connectivité

« La maîtrise du routage au cœur des backbones mondiaux permet de nous assurer de l'étanchéité réelle entre le VPN de nos client et l'Internet. Cette étanchéité ne peut jamais être garantie et doit donc être pilotée et monitorée au cœur des réseaux »

C'est pourquoi Orange Business propose une offre de Cloud connectivité. Elle apporte en premier lieu des garanties de qualité de service pour le trafic sensible. Elle permet aussi et surtout d'apporter le réseau privé de notre client (VPN) au cœur de la plateforme, comme si l'infrastructure Cloud de confiance était sur le site client. Les données sensibles, hébergées dans un Cloud de confiance sont donc également protégées tout au long de leur transport jusqu'à l'utilisateur.

>>

Ceci est possible avec le déploiement par Orange de notre cœur de réseau dans les datacenters de Bleu. Cette interconnexion directe nous permet de maîtriser et superviser l'ensemble des flux entrants et sortants de l'environnement client. Cet équipement cœur de réseau est aussi rendu étanche à l'Internet et garantit ainsi un cloisonnement strict à l'intérieur du VPN client. Cet équipement et le transport des données, gérés par Orange uniquement (*entreprise à capital Français et apportant les garanties d'immunité aux lois extra territoriales américaines*) combiné aux datacenters qui hébergent les données, gérés par Bleu uniquement, est la garantie d'un « continuum de souveraineté » pour la donnée client.

Franck Lehr - Expert Opérations de Confiance

« L'installation d'équipements de chiffrement entre les sites clients et les datacenters de Bleu permet de garantir un trafic « noir » sur le réseau Orange. Les données les plus sensibles (DR ou SIIV) transitent de bout en bout avec une confidentialité garantie et certifiée par l'ANSSI ».

Au-delà de ces garanties techniques et opérationnelles, Orange Business peut aussi proposer aux clients les plus exigeants ou faisant face à des réglementations spécifiques type II901 ou LPM de réaliser du chiffrement de bout en bout au travers d'équipements certifiés par l'ANSSI et gérés par des personnels habilités. Ainsi, le contenu du trafic est invisible de bout en bout pour l'opérateur.

Liste des contributeurs

Emmanuel Cacheux
Chief Trust Officer
Orange Business

Géraldine Steinberg
Chief Partner Officer
Orange Business

Études, Conseil

Guillaume Grard
Directeur d'Orange Consulting

Thierry Hamelin
Senior Manager
Conseil Move to Bleu
thierry.hamelin@orange.com
Orange Consulting

Thierry Gluzman
Senior Manager CIO Advisory
thierry.gluzman@orange.com
Orange Consulting

Amina Bensetti
Manager IT & Réseau
amina.bensetti@orange.com
Orange Consulting

Pierrick Besson
Directeur Conseil Modern Workplace
pierrick.besson@orange.com
Orange Consulting

Jean-Michel Menant
Directeur Expérience Employés
jeanmichel.menant@orange.com
Orange Consulting

Applications de productivité

Pierre-Emmanuel Duc
Business Developer, Expert Microsoft et Bleu
pierreemmanuel.duc@orange.com
Orange Business

Eliott Vernières
Ingénieur Avant-Vente, Expert Microsoft et Bleu
eliott.vernieres@orange.com
Orange Business

Cybersécurité

Sébastien De Lattin
Responsable de la Business Unit Microsoft Security
sebastien.delattin@orange.com
Orange Cyberdefense

Axel Beiner
Responsable Sécurité du Cloud au sein de la Business Unit Conseil & Audit
axel.beiner@orange.com
Orange Cyberdefense

Infrastructure et applications

Alexandre Saker
Senior Architect Microsoft Azure et Bleu
alexandre.saker@orange.com
Orange Business

Matthieu Petite
Senior Architect Microsoft Azure et Bleu
matthieu.petite@orange.com
Orange Business

Jonathan Jehanno
Senior Architect Microsoft Azure et Bleu
jonathan.jehanno@orange.com
Orange Business

Connectivité

Antoine Soubigou
Architecte Cloud Connectivité
antoine.soubigou@orange.com
Orange Business

Franck Lehr
Expert Opérations de Confiance
franck.lehr@orange.com
Orange Business

Merci à Laurent Lemaire, Directeur Commercial, Marketing et Partenariats de Bleu