OPCP

On-Prem Cloud Platform

Résilience. Contrôle. Continuité.

Un socle technologique moderne maîtrisé, industrialisé et sécurisé, conçu pour garantir la continuité des services essentiels et la protection des actifs stratégiques.

Les Organismes d'Importance Vitale (OIV) : le socle stratégique d'une nation

Dans chaque pays, **les Organismes d'Importance Vitale (OIV)** constituent l'ossature opérationnelle de la nation. Ils regroupent les entités publiques ou privées dont l'interruption, la défaillance ou la compromission aurait un impact direct et massif sur la sécurité nationale, la stabilité économique ou la continuité des services essentiels à la population.

Un OIV se caractérise par son rôle stratégique dans le fonctionnement du pays et par sa contribution directe à la continuité des services essentiels, bien au-delà des seuls indicateurs économiques. Lorsqu'un opérateur énergétique cesse de fonctionner, ce sont les hôpitaux, les transports, les entreprises et les administrations qui sont affectés. Lorsqu'un système financier national est perturbé, c'est l'ensemble de l'économie qui ralentit. Lorsqu'un réseau de télécommunications est compromis, la coordination des services publics et privés devient fragile.

Les secteurs concernés — énergie, eau, télécommunications, transports, finance, santé, infrastructures numériques, industrie stratégique — assurent le fonctionnement quotidien d'un État moderne. Ils soutiennent les activités économiques, garantissent la sécurité des citoyens, permettent l'exercice des missions régaliennes et structurent la compétitivité nationale.

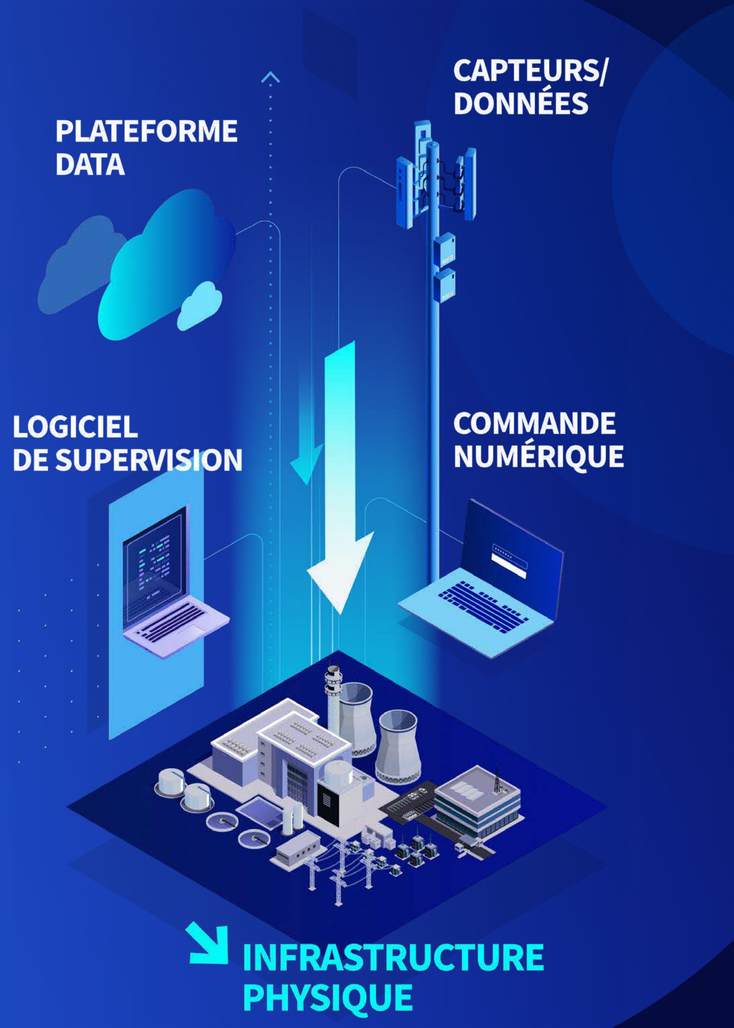
La performance des OIV dépasse la seule efficacité opérationnelle. Elle influence directement :

- la **confiance des citoyens** envers les institutions,
- la **crédibilité internationale** du pays,
- l'**attractivité économique** auprès des investisseurs,
- la **résilience face aux crises**, qu'elles soient sanitaires, climatiques, économiques ou géopolitiques.

Un OIV n'est pas une organisation comme les autres. Elle porte une responsabilité systémique.

Sa robustesse ou sa fragilité peut produire des effets en chaîne sur l'ensemble du territoire. Elle agit comme un multiplicateur de stabilité… ou de vulnérabilité. C'est pourquoi sa gouvernance, son architecture technologique et son niveau de protection ne peuvent être considérés comme de simples choix techniques.

Ils relèvent d'une responsabilité stratégique, à la fois économique et nationale.



La protection du numérique des OIV : un enjeu de souveraineté globale

La numérisation massive des infrastructures critiques a profondément redéfini le rôle et la nature même des OIV. Les réseaux industriels autrefois cloisonnés sont désormais connectés. Les systèmes de supervision s'appuient désormais sur des architectures numériques intégrées et interconnectées. Les décisions opérationnelles reposent sur l'exploitation de données en temps réel. L'automatisation, l'orchestration logicielle et l'intégration d'algorithmes d'intelligence artificielle sont devenues des standards.

Cette transformation a permis des gains considérables en performance, en efficacité énergétique, en capacité de pilotage et en anticipation des incidents. Les OIV sont aujourd'hui capables d'optimiser leurs opérations, de mieux prévoir les fluctuations de demande, d'améliorer la maintenance prédictive et de renforcer la qualité de service.

Mais cette modernisation s'accompagne d'une nouvelle réalité : **l'exposition accrue au risque numérique.**

Les infrastructures physiques — centrales électriques, réseaux de transport, systèmes financiers, réseaux télécom — sont désormais indissociables de leurs couches logicielles.
Une vulnérabilité informatique peut produire un effet direct sur le monde réel.
Les infrastructures critiques évoluent désormais dans un environnement de convergence cyber-physique. Les systèmes numériques pilotent des actifs industriels, énergétiques ou logistiques réels.

Maîtriser cette convergence devient essentiel pour éviter qu'une vulnérabilité logicielle ne se traduise en impact physique sur le territoire.

Une sécurité qui dépasse la simple protection informatique

Dans ce contexte, la sécurité des OIV dépasse largement la simple protection informatique. Elle engage la capacité d'un État à :

- maintenir l'ordre public,
- garantir l'accès aux services essentiels,
- préserver la stabilité économique,
- protéger ses intérêts stratégiques face à des menaces hybrides.

Une attaque réussie contre une infrastructure énergétique peut entraîner des coupures massives.Une compromission d'un système financier peut bloquer des paiements à l'échelle nationale.Une perturbation des réseaux télécom peut désorganiser la coordination des services d'urgence et des institutions publiques.

Les effets sont immédiats, systémiques et potentiellement transnationaux.
La robustesse numérique des OIV est ainsi devenue un pilier de la stabilité géopolitique. Elle influence la capacité d'un pays à résister aux pressions extérieures, à absorber des chocs majeurs et à maintenir la confiance des citoyens et des partenaires internationaux.

Un cadre réglementaire et normatif de plus en plus structurant

Cette évolution s'inscrit dans un environnement réglementaire et normatif en forte consolidation. Les États et les régulateurs élèvent progressivement le niveau d'exigence applicable aux infrastructures critiques, reconnaissant leur rôle central dans la stabilité économique et la sécurité collective.

Des dispositifs comme **NIS2 en Europe, DORA pour le secteur financier** ou les standards industriels tels qu'**IEC 62443** traduisent une exigence commune : renforcer la cybersécurité, formaliser la résilience opérationnelle et maîtriser les risques systémiques.

Pour les OIV, la conformité ne relève plus d'une simple obligation réglementaire. Elle devient un cadre structurant qui impose d'intégrer la résilience, la gouvernance des risques et la souveraineté numérique dès la conception des architectures.

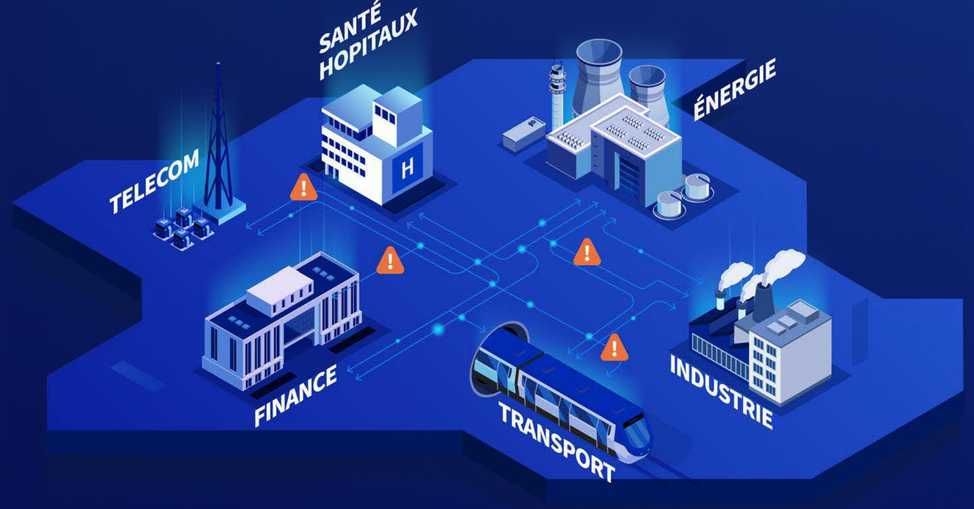
Dès lors, le développement continu des capacités numériques des OIV ne peut être envisagé uniquement sous l'angle de la performance technologique. Il doit intégrer, dès sa conception, les exigences de résilience, de souveraineté et de continuité absolue.

Des vulnérabilités accrues dans un monde interconnecté et structurellement instable

Les OIV évoluent dans un contexte de menaces permanentes, sophistiquées et ciblées, où les infrastructures critiques sont devenues des points stratégiques à fort impact de nuisance.

Les cyberattaques ne visent plus seulement les données : elles ciblent directement les opérations physiques.

La convergence IT/OT a estompé la frontière entre monde numérique et monde physique, exposant directement les opérations critiques aux risques cyber et imposant **des architectures segmentées et des modèles Zero Trust pour limiter les risques de propagation.**



Un risque systémique

Les OIV forment un système interconnecté : énergie, télécommunications, finance, transport et industrie sont interdépendants.
Une défaillance isolée peut provoquer un effet domino à l'échelle nationale.

Les vulnérabilités résident désormais dans :
- les dépendances technologiques partagées,
- les chaînes d'approvisionnement logicielles,
- les interconnexions numériques entre secteurs,
- les architectures fragmentées.

La dépendance technologique devient un risque stratégique, amplifiant les effets de cascade ("cascading failures").

L'enjeu clé

De nombreux OIV reposent encore sur des systèmes complexes, anciens et fortement interdépendants. Toute évolution comporte un risque opérationnel, alors même que la tolérance à l'interruption est quasi inexistante.

Le défi n'est donc pas seulement de se protéger, mais de faire évoluer les infrastructures sans fragiliser l'existant.

Il s'agit de renforcer la résilience tout en poursuivant l'évolution technologique, dans un cadre maîtrisé, progressif et compatible avec les impératifs de continuité d'activité.

La résilience doit désormais être pensée de manière systémique, à l'échelle de l'écosystème national.

Autonomie stratégique numérique : répondre à une équation sous contrainte permanente

Pour les dirigeants d'OIV, la gestion des infrastructures critiques repose sur une équation exigeante : garantir une **disponibilité permanente**, renforcer la cybersécurité, faire évoluer des systèmes complexes sans interrompre l'exploitation, maîtriser les investissements et réduire les dépendances technologiques stratégiques.

Chaque évolution doit préserver la continuité d'activité et ne jamais fragiliser les opérations en cours.

La résilience ne peut plus se limiter à des plans théoriques. Elle devient un processus opérationnel continu, intégré dès la conception des infrastructures ("resilience by design") : scénarios testés, exercices de crise, plans de reprise automatisés et vérifiables.

Dans un contexte de pression budgétaire croissante, la performance technologique est indissociable de la performance économique. Les OIV doivent concilier résilience et maîtrise des coûts, optimiser les ressources critiques et garantir une prévisibilité budgétaire durable.

Dans ce cadre, l'autonomie stratégique numérique s'impose comme la condition de cette maîtrise.

Elle signifie la capacité concrète de choisir où sont hébergées les données, comment elles sont gouvernées, qui y accède et selon quelles règles juridiques. Elle implique la maîtrise des infrastructures, la limitation des dépendances critiques, la réversibilité des architectures et la possibilité d'adapter le modèle d'exploitation en fonction des contraintes réglementaires, opérationnelles ou géopolitiques.

L'autonomie n'est pas un repli : c'est la capacité à décider et à évoluer sous contrôle. Elle devient le levier structurant qui permet d'innover, d'intégrer les technologies modernes et de moderniser durablement les infrastructures critiques sans perdre la maîtrise stratégique.

Les limites d'un modèle exclusivement fondé sur le cloud conventionnel

Le cloud conventionnel a profondément transformé les modèles informatiques. Il apporte souplesse, élasticité et rapidité de déploiement. Il permet d'industrialiser les environnements, d'optimiser certaines charges de travail et d'accélérer l'innovation applicative.

Cependant, pour un OIV, il ne peut constituer l'unique fondation technologique. Certaines données stratégiques — énergétiques, financières, industrielles, sanitaires — ne peuvent quitter un périmètre strictement maîtrisé, souvent national. **Leur sensibilité impose un contrôle total sur leur localisation, leurs accès et leur cycle de vie.**

De nombreux environnements critiques doivent également continuer à fonctionner en cas de rupture de connectivité, de crise majeure ou d'isolement volontaire. **Une infrastructure dépendante d'un accès permanent à des ressources externes peut devenir un point de fragilité.** Or, pour un OIV, la continuité d'activité n'est pas négociable.

Enfin, **certains traitements nécessitent un isolement complet :** environnements classifiés, systèmes industriels sensibles, plateformes stratégiques. Ces contextes sont difficilement compatibles avec des architectures mutualisées ou partagées.

Les infrastructures vitales ont donc besoin d'un modèle hybride maîtrisé : un modèle capable d'intégrer les bénéfices des technologies cloud — automatisation, standardisation, agilité — tout en les inscrivant dans un cadre de contrôle strict, souverain et résilient qu'offrent les infrastructures on-premise.

Au-delà des infrastructures, le risque s'étend désormais à la chaîne d'approvisionnement logicielle. Dépendance à des composants tiers, vulnérabilités embarquées, mises à jour non maîtrisées : **la gestion des risques fournisseurs et la traçabilité des composants logiciels (logique SBOM) deviennent un enjeu stratégique pour les infrastructures critiques.**

L'enjeu n'est donc pas de renoncer à l'innovation, mais de l'ancrer dans une architecture compatible avec les exigences d'une mission critique.

Moderniser les infrastructures vitales sans compromettre la souveraineté : l'approche OPCP

OPCP est une plateforme cloud on-premise conçue pour répondre aux exigences des environnements critiques. Elle apporte les capacités d'un cloud moderne tout en restant intégralement déployée et contrôlée au sein des infrastructures de l'organisation.

Elle permet **d'automatiser les déploiements, de standardiser les environnements multi-sites, de renforcer la sécurité par conception et d'assurer une gouvernance centralisée.** Surtout, elle fonctionne dans toutes les configurations : data centers nationaux, sites industriels distants, environnements Edge ou installations air-gap totalement isolées.

OPCP ne remplace pas les infrastructures existantes du jour au lendemain. Elle les modernise progressivement et les structure autour d'un socle cohérent et résilient. Les environnements historiques peuvent coexister avec des services cloud-native, dans un cadre structuré et sécurisé. La transformation devient continue, maîtrisée et compatible avec les impératifs de continuité d'activité.

Lorsque cela est pertinent, OPCP peut également s'inscrire dans une logique d'extension vers des environnements SNC OVHcloud, reposant sur le même socle technologique. Cette continuité garantit la portabilité et la réversibilité des charges de travail, sans compromis sur la maîtrise des environnements critiques.

La réponse OPCP : une architecture souveraine conçue pour les environnements critiques

OPCP apporte aux OIV un socle technologique moderne, tout en garantissant un contrôle total des données, des accès et des opérations.

OPCP combine ainsi :

- la puissance et l'agilité d'un cloud moderne
- la maîtrise et la souveraineté du on-premise
- une automatisation complète de l'infrastructure
- une gouvernance fine multi-entités
- la capacité à fonctionner en Edge ou en environnement air-gap
- une résilience native adaptée aux missions critiques

OPCP constitue un socle technologique unifié, industrialisé et gouverné, pensé pour accompagner l'évolution des systèmes critiques tout en assurant continuité, maîtrise et souveraineté.

LANDING ZONE MANAGER

Gouvernance stratégique et segmentation maîtrisée
- Isolation par entité, par mission ou par niveau de sensibilité.
- Gestion des rôles, quotas et politiques de conformité.
- Supervision centralisée ou distribuée.

Il permet d'opérer un environnement multi-sites complexe sans perdre le contrôle stratégique.

CLOUD STORE

Déploiement rapide et standardisé des services critiques.
- Machines virtuelles, bases de données, plateformes analytiques, moteurs IA, outils métiers sensibles.
- Déploiement possible en datacenter central, en site distant ou en environnement isolé.

Il accélère les projets tout en respectant les exigences de sécurité et de conformité.

OPCP CORE

Le socle technique automatisé et résilient.
- Orchestration complète du calcul, du stockage, du réseau et de la sécurité.
- Observabilité avancée et mises à jour automatisées.
- Fonctionnement possible en site déconnecté ou sous contraintes fortes.

Il constitue la fondation souveraine sur laquelle reposent toutes les opérations critiques.

OPCP : un socle souverain pour répondre aux exigences des OIV

Les OIV évoluent sous des contraintes opérationnelles, réglementaires et géopolitiques spécifiques. Leur transformation numérique doit simultanément garantir continuité, résilience, maîtrise économique et autonomie stratégique.

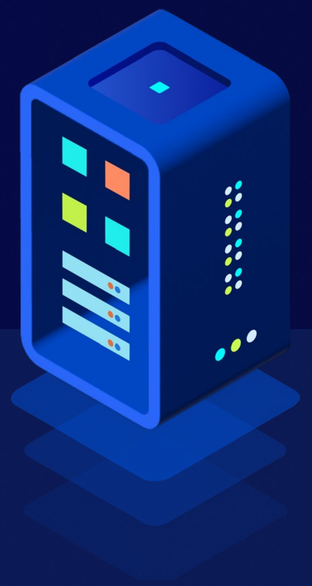
OPCP répond à cette équation en fournissant un socle technologique unifié, maîtrisé et industrialisé, conçu pour les environnements critiques.

OPCP permet aux OIV de :

- **assurer une continuité d'activité absolue**, y compris en environnement isolé, multi-sites ou sous contrainte forte,
- **renforcer la résilience by design**, grâce à une automatisation complète, une segmentation fine et une gouvernance centralisée,
- **maîtriser la localisation et la gouvernance des données,** dans le respect des exigences réglementaires et de souveraineté,
- **réduire les dépendances technologiques critiques,** en conservant le contrôle des infrastructures et des architectures,
- **optimiser les ressources et les coûts,** en standardisant les environnements et en mutualisant les capacités stratégiques,
- **moderniser progressivement les systèmes existants,** sans rupture opérationnelle.

OPCP n'est pas un simple outil d'infrastructure. **Il constitue un cadre d'exploitation stratégique permettant aux OIV d'évoluer, d'innover et de se protéger sans compromettre leur mission essentielle.**

Les cas d'usage suivants illustrent concrètement comment OPCP répond aux enjeux réels des OIV dans des environnements sous contrainte opérationnelle forte.



OPCP

USE CASE | **01**

Modernisation et sécurisation du SI d'un opérateur énergétique

Moderniser un système d'information critique sous contrainte de continuité et de cybermenace.

Les opérateurs énergétiques nationaux s'appuient sur des systèmes d'information complexes : supervision industrielle (SCADA/OT), gestion du réseau, applications métiers, maintenance et outils analytiques.La transition énergétique et la digitalisation des opérations ont multiplié les flux de données et renforcé les interconnexions IT/OT.
Parallèlement, les attaques ciblant le secteur énergétique se sont intensifiées. Les systèmes historiquement isolés sont désormais interconnectés et exposés, augmentant le risque opérationnel.

OPCP permet :

- → d'**unifier et sécuriser l'infrastructure** IT et OT autour d'un socle maîtrisé,
- → d'**isoler strictement les environnements** critiques par segmentation,
- → d'**héberger localement** les données et applications sensibles,
- → d'**assurer la continuité d'activité** en cas de crise ou de rupture réseau,
- → de **moderniser progressivement le SI** sans interruption d'exploitation.

OPCP permet à l'opérateur énergétique de sécuriser et faire évoluer son système d'information tout en garantissant la continuité des opérations et la résilience nationale.

OPCP

USE CASE | **02**

Résilience d’un système national de paiement

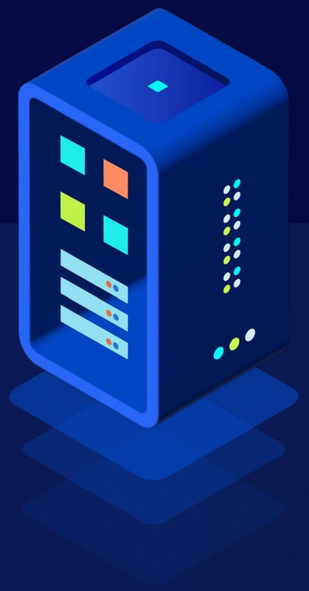
Garantir la continuité financière en cas de cyberattaque majeure.

Les systèmes interbancaires nationaux traitent des volumes massifs de transactions en temps réel. Une interruption, même de courte durée, peut affecter l’économie nationale et la confiance des marchés. Les menaces cyber ciblant les institutions financières se sont intensifiées, notamment via des attaques par déni de service ou compromission de systèmes critiques.

OPCP permet :

- de **déployer une architecture multi-sites** résiliente,
- d’**isoler les traitements critiques** dans des environnements segmentés,
- de **maintenir des capacités locales** en cas de rupture réseau,
- de **garantir la traçabilité** complète des accès et des opérations,
- d’**assurer une reprise rapide** après incident.

OPCP renforce la stabilité du système financier en assurant une continuité d’activité souveraine et maîtrisée.



OPCP

USE CASE | **03**

Gestion sécurisée d'un réseau national d'eau potable

Garantir la continuité d'approvisionnement et la surveillance sanitaire.

Les opérateurs d'eau gèrent des infrastructures distribuées : stations de pompage, usines de traitement, réseaux de distribution, systèmes de contrôle qualité.Ces installations reposent sur des capteurs, des systèmes industriels et des plateformes de supervision inter connectées.

Une altération, qu'elle soit cyber ou physique, peut affecter directement la santé publique et la stabilité sociale.

OPCP permet :

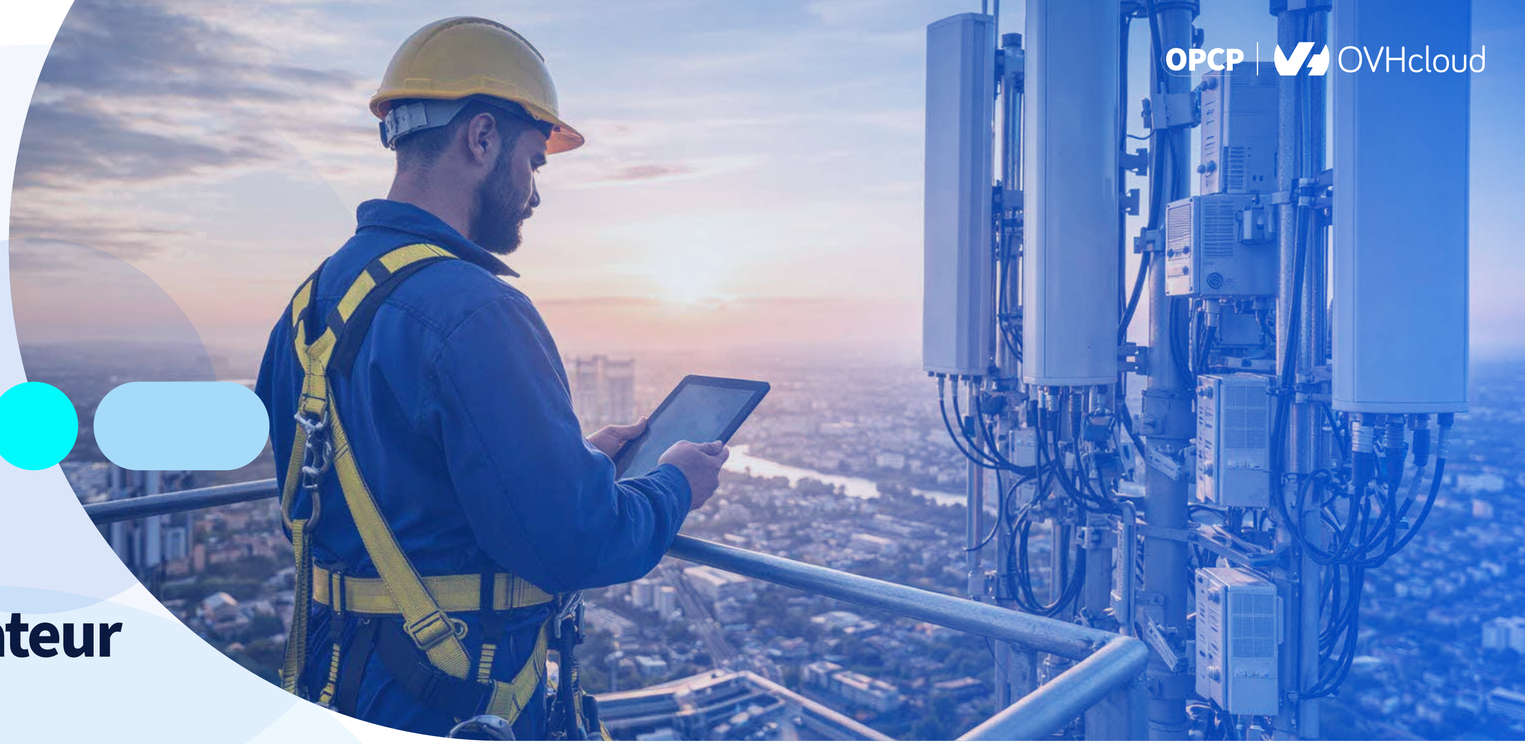
- de **sécuriser les systèmes de supervision** industrielle,
- d'**isoler les environnements** sensibles par zone géographique,
- de **déployer des capacités Edge** sur des sites distants,
- d'**analyser en temps réel les données** de qualité de l'eau dans un cadre souverain,
- de **garantir la continuité opérationnelle** même en situation dégradée.

OPCP offre au réseau d'eau un socle résilient permettant d'assurer la sécurité sanitaire et la continuité d'un service vital.

OPCP

USE CASE | **04**

Sécurisation d'un opérateur télécom stratégique



Maintenir la disponibilité des réseaux nationaux sous contrainte.

Les opérateurs télécom nationaux sont devenus des infrastructures critiques. Leur indisponibilité peut affecter les services d'urgence, la coordination gouvernementale et l'économie numérique.
Les environnements sont distribués, hétérogènes et fortement sollicités.

OPCP permet :

- de **déployer des capacités Edge** sécurisées sur les nœuds régionaux,
- d'**automatiser la gestion des infrastructures** multi-sites,
- d'**isoler les environnements sensibles**,
- d'**assurer une supervision** unifiée et centralisée,
- de **maintenir des opérations locales** même en cas d'isolement.

OPCP renforce la robustesse opérationnelle d'un réseau télécom national sous contrainte permanente.

OPCP

USE CASE | **05**

Industrie stratégique et environnement classifié

Déployer des capacités avancées en environnement air-gap.

Les industries stratégiques et les environnements de défense manipulent des données classifiées.Certaines infrastructures doivent fonctionner en isolement total, sans connexion externe.
Ces environnements nécessitent néanmoins des capacités modernes : IA, simulation, calcul intensif.

OPCP permet :

- de **déployer une infrastructure** complète en environnement air-gap,
- de **mutualiser des ressources** GPU ou compute avancées localement,
- d'**assurer une segmentation stricte** par niveau de classification,
- d'**automatiser les déploiements** sans dépendance externe,
- de **conserver une gouvernance centralisée** tout en respectant l'isolement.

OPCP permet d'allier modernité technologique et souveraineté absolue dans les environnements les plus sensibles.

OPCP

USE CASE | **06**

Résilience d'un système national de transport ferroviaire

Assurer la continuité des flux voyageurs et marchandises.

Les réseaux ferroviaires nationaux reposent sur des systèmes de signalisation, de gestion du trafic, de billetterie et de supervision en temps réel.Ces environnements sont fortement interconnectés, distribués et soumis à des exigences strictes de disponibilité.
La modernisation vers des systèmes numériques avancés (IoT, maintenance prédictive, gestion intelligente du trafic) augmente la surface d'exposition cyber.

OPCP permet :

- d'**unifier l'infrastructure** entre centres de contrôle et sites régionaux,
- de **segmenter strictement les systèmes** critiques de signalisation,
- de **déployer des capacités Edge** sur les hubs opérationnels,
- d'**assurer une haute disponibilité** multi-sites,
- de **moderniser les applications historiques** sans perturber l'exploitation.

OPCP permet au système ferroviaire national de gagner en efficacité, en sécurité et en résilience sans compromettre la continuité du service public.

Une complémentarité qui a du sens

D'un côté, une solution technique éprouvée.
De l'autre, une connaissance fine du terrain.
Il est clair qu'il y a des choses à faire ensemble.

Des cas à inventer, adapter, tester

Les cas d'usage ne manquent pas : edge, usines, sites critiques, infrastructures déconnectées…
Et si on en identifiait un ou deux pour avancer concrètement ?

Un atelier, un échange, un POC ?

Pas besoin de tout figer d'emblée.
Juste un moment pour creuser ensemble,
voir ce qui a du sens, et construire, pas à pas.

ovhcloud.com
opcp@ovhcloud.com