OPCP

On-Prem Cloud Platform

Resilience. Control. Continuity.

A secure, industrialised, and expertly managed modern technological base, built to ensure the continuity of essential services and protect strategic assets.

Operators of Essential Services (OES): a nation's strategic foundation

Operators of Essential Services (OES) serve as the operational backbone of every nation. They are public or private entities whose discontinuity, failure, or compromise would significantly and widely affect national security, economic stability, or the delivery of essential public services.

An OES is defined by its strategic role in national operations and its contribution to the uninterrupted delivery of essential services — which extends far beyond simple economic indicators. When an energy operator is disrupted, the ripple effects are felt across hospitals, transport networks, businesses, and administrative offices. The entire economy grinds to a halt when a national financial system is disrupted. When a telecommunications network is disrupted, coordination between public and private services is weakened.

The sectors involved — energy, water supply, telecom, transport, finance, public health, digital infrastructure, strategic industries — are crucial for a country's daily operations. They bolster economic activities, ensure public safety, facilitate the performance of sovereign duties, and reinforce a nation's competitive standing.

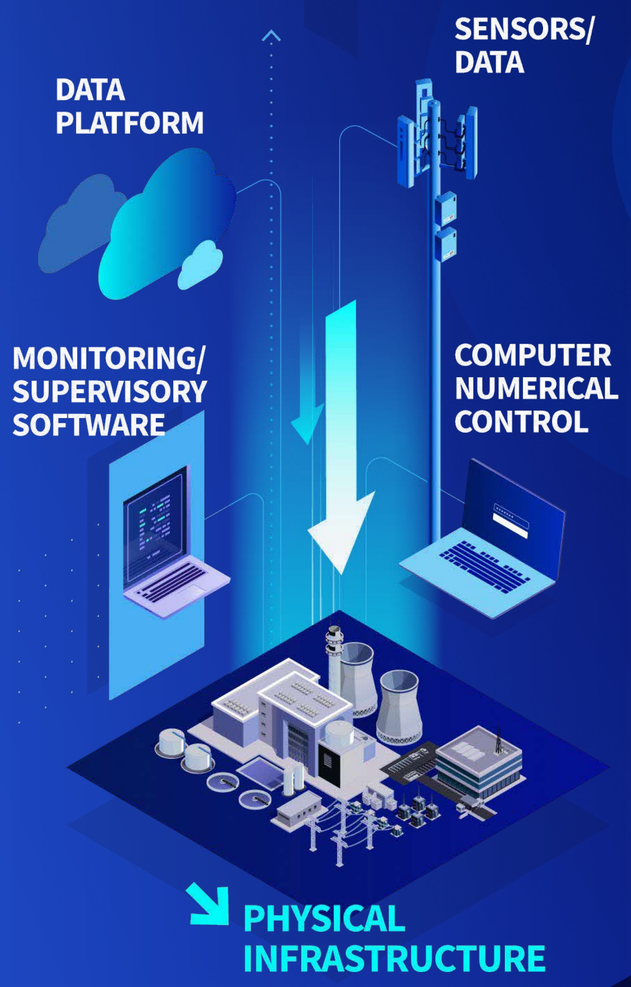
The role of OESs encompasses more just operational efficiency. It has a direct bearing on:

- **the public's trust** in institutions
- a country's **credibility on the international stage**,
- a country's **economic attractiveness** to investors,
- a country's **resilience during crises**, whether they stem from health issues, climate change, economic downturns, or geopolitical instability.

An OES isn't just any organisation; it plays a key role in a nation's operational continuity.

Its strength
or weakness can have far-reaching impacts on a country. OESs have the potential to either boost stability or exacerbate vulnerability. As a result, their administration, technological design, and security shouldn't be viewed as purely technical.

They are important because of a strategic necessity that is both economic and national in scope.



Protecting the digital infrastructure of OESs: a matter of global sovereignty

The extensive digitisation of essential services has fundamentally transformed OESs and their role. Previously isolated industrial networks are now interconnected, with monitoring systems relying on integrated and linked digital architectures. Operational decisions are informed by the use of live data, with automation, software orchestration, and the integration of AI algorithms now becoming standards.

This shift allows for significant improvements in performance, energy efficiency, control capabilities, and the ability to anticipate issues. OESs can now optimise their operations, more accurately forecast changes in demand, improve predictive maintenance capabilities, and elevate service quality.

The flipside of this modernisation is a new reality: **increased exposure to digital risk.**

Physical infrastructures — power plants, transport networks, financial systems, telecom networks — are now inseparable from their software layers.
A weak cybersecurity posture could have tangible, real-life consequences.
Critical infrastructures are evolving within an increasingly convergent cyber-physical environment, where digital systems manage industrial, energy, or logistical assets.

Successfully managing this convergence is crucial to ensure software vulnerabilities don't lead to real-world consequences nationwide.

Security that extends beyond basic IT defences

OES security, in this context, is much more important than standard IT security. It enables a country to:

- maintain public order,
- guarantee access to essential services,
- protect economic stability,
- shield its strategic interests from hybrid threats.

An attack on energy infrastructure could trigger widespread power outages, while a breach of financial systems might halt national payments. Furthermore, disruptions to telecom networks could lead to a chaotic breakdown in the coordination of essential public services and emergency response.

The consequences are immediate, impacting the entire nation and potentially extending to other countries.
As a result, the digital strength of OESs has become a cornerstone of geopolitical stability. It bolsters a country's resilience against external pressures, its capacity to bounce back from major setbacks, and its ability to maintain the trust of its citizens and international partners.

An increasingly structured framework of regulations and standards

This shift is happening as regulations and standards are becoming increasingly stringent. Recognising the central role of OESs in economic stability and national security, authorities and regulatory bodies are gradually raising the standards for critical infrastructures.

The **NIS2 EU directive, DORA (for finance institutions)**, and industrial standards (such as **IEC 62443**) all point to a common need for enhanced cybersecurity, structured operational resilience, and better management of systemic risks.

As a result, OESs now view compliance as more than just a legal responsibility. It has become foundational, requiring resilience, risk governance, and digital sovereignty right from the initial stages of architectural design.

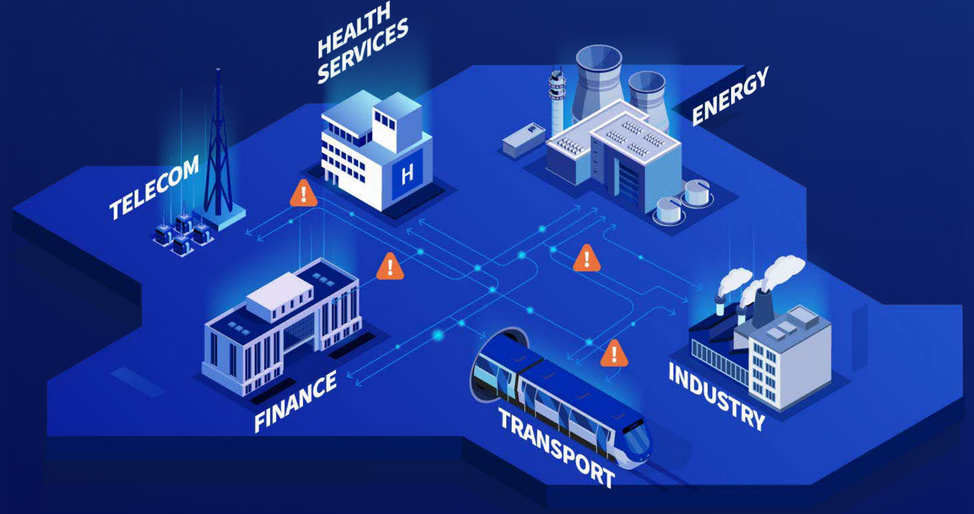
In light of this, the development of an OES's digital skills shouldn't be assessed solely based on technological achievements. It needs to be designed from the ground up with resilience, sovereignty, and enhanced continuity in mind.

Heightened risks in a connected but fragile global landscape

Critical infrastructures have become prime targets for causing significant disruption to an OES's operational sphere, characterised by persistent, advanced, and deliberate threats.

Cyberattacks now impact more than just data, directly affecting physical operations.

The integration of IT and OT has blurred the lines between digital and physical environments, leaving essential operations vulnerable to cyber threats, and requiring **segmented architectures and Zero Trust models to prevent the spread of risk.**



A systemic risk

Energy, telecommunications, finance, transport, and industry are all interdependent, highlighting the interconnected nature of OESs.
An isolated failure could trigger a domino effect on a national scale.

Vulnerabilities can now be found in:
- shared technological dependencies,
- software supply chains,
- cross-sector digital connections,
- fragmented architectures.

Dependence on technology is becoming a major strategic threat, setting off widespread system breakdowns.

The key issue

Many OESs still rely on complex, outdated, and highly interdependent systems. Any change introduces operational risk, particularly because there's almost no room for disruption.

The challenge is therefore not just self-protection, but modernising infrastructure without compromising existing systems.

It's building resilience and supporting technological advancement through a carefully managed, phased process that aligns with business continuity requirements.

As a result, resilience should be viewed as an integral part of the entire national ecosystem.

Navigating the complexities of digital strategic autonomy amidst ongoing constraints

OESs face a challenging task in managing critical infrastructures, which requires achieving **continuous availability**, improving cybersecurity, seamlessly modernising complex systems, controlling costs, and reducing dependence on critical technologies.

Every change should ensure operational continuity without disrupting ongoing tasks.
Instead of remaining theoretical, resilience becomes a continuous operational process. This means building it in from the start of infrastructure design, a concept known as ‘resilience by design’. Key elements include tested scenarios, crisis simulations, and recovery plans that are both automated and verifiable.

As budget pressures mount, technology performance can’t be separated from its economic impact. OESs need to balance resilience, cost control, efficient use of critical resources, and long-term budget predictability.

Here, digital strategic autonomy is the basis upon which this control can be achieved.

Essentially, it’s the practical ability to choose where data is hosted, how it’s governed, who has access, and under what laws and regulations. This requires understanding infrastructure, reducing critical dependencies, making architectures reversible, and adjusting operating models to suit regulatory, operational, or geopolitical factors.

Autonomy isn’t about giving up; it’s about having the ability to make choices and grow with full control. It has become fundamental to innovation, the integration of modern technologies, and ongoing modernisation of critical infrastructures without giving up strategic control.

The limits of a purely traditional cloud-based model

Traditional cloud technology has revolutionised how we compute; it ensures flexibility, elasticity, and rapid deployment. It also supports the deployment of large-scale environments, the optimisation of specific workloads, and faster application development.

On its own, this technology can't stand as the sole technological foundation for an OES. Some strategic data — energy, financial, industrial, health — is restricted from leaving a tightly managed zone, typically a national border. **Their sensitive nature requires total control over their location, access, and lifecycle.**

Many essential services need to stay up and running — regardless of connectivity issues, major crises, or voluntary isolation situations.

Ongoing reliance on external assets can expose operations to potential vulnerabilities. More precisely, business continuity for an OES is non-negotiable.

Certain processes need complete isolation, particularly in classified environments, sensitive industrial systems, and on strategic platforms. These scenarios are hardly compatible with shared infrastructures or pooled resources.

That's why critical infrastructure benefits from a tightly controlled hybrid model. This model combines the benefits of cloud technologies — automation, standardisation, agility — with the robust, sovereign, and uncompromised control of on-premises infrastructures.

Today, the risk extends beyond existing infrastructure to include the software supply chain. For critical infrastructures, **handling supplier risks and maintaining full traceability of software components (using SBOMs) is now a strategic priority**. This is due to issues such as dependence on third-party components, embedded vulnerabilities, and unmonitored updates.

The difficulty, then, lies not in abandoning innovation, but in anchoring it within an architecture that meets the demands of essential services.

The OPCP approach: modernising critical infrastructures without compromising sovereignty

OPCP is an on-premises cloud platform, built to handle the demands of crucial operational environments. It brings modern cloud capabilities into an organisation's infrastructure to ensure full control.

This system facilitates **automated deployments, standardises multi-site setups, enhances security from the ground up, and ensures centralised governance.**
Above all, it can work in any setup: national datacentres, remote industrial sites, edge systems, or completely isolated air-gapped environments.

OPCP doesn't replace existing infrastructures overnight, but rather it gradually updates existing infrastructures and builds them upon a unified and resilient foundation.

Older, established systems integrate seamlessly with cloud-native services, all protected by a well-defined and secure structure. Transformation becomes an ongoing, managed process that aligns with the need to keep critical environments operational.

When relevant, OPCP can also extend to OVHcloud SNC environments, utilising the same technological base. This continuity supports the portability and reversibility of workloads, while maintaining control over crucial systems.

The OPCP strategy: sovereign architecture designed for critical setups

OPCP provides OESs with a modern technological base, while ensuring complete control over data, access, and operations.

As a result, OPCP brings:

- the power and agility of a modern cloud,
- the control and sovereignty of an on-site setup,
- complete infrastructure automation,
- fine-grained governance across organisations,
- the ability to operate in edge or air-gapped environments,
- cloud-native resilience suited for critical operations.

With its unified, industrialised, and governed foundation, OPCP is designed to support critical system updates, and ensure continuity, efficiency, and autonomy.

LANDING ZONE MANAGER

Strategic governance and controlled segmentation.

- Isolation by entity, mission, or level of sensitivity
- Roles, quotas, and compliance management
- Centralised or distributed oversight

Landing Zone Manager ensures the management of multiple complex environments, without giving up strategic control.

CLOUD STORE

Rapid and standardised deployment of critical services.

- Virtual machines, databases, analytics platforms, AI engines, or sensitive business tools
- Deployment in a central datacentre, at a remote site, or within an isolated setup

Cloud Store speeds up projects while complying with security and compliance regulations.

OPCP CORE

An automated and resilient underlying infrastructure.

- Complete compute, storage, network, and security orchestration
- Advanced observability and automated updates
- Operational capability in offline environments or under stringent conditions

OPCP forms the sovereign foundation underpinning all critical operations.

OPCP: a sovereign foundation to meet the requirements of OESs

Because OESs operate under specific operational, regulatory, and geopolitical constraints, their digital transformation needs to balance continuity, resilience, economic control, and strategic autonomy.

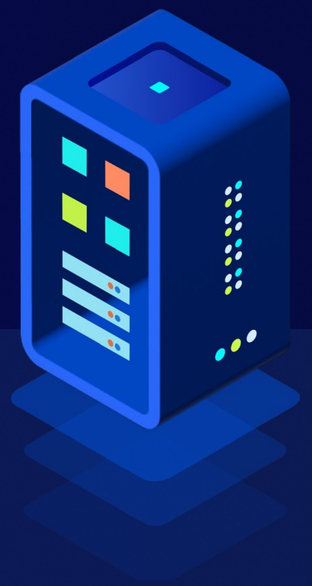
OPCP tackles this problem by offering a unified, regulated, and industrialised technological foundation — engineered for critical environments.

OPCP enables OESs to:

- **maintain total business continuity**, including in isolated, distributed, or highly restricted setups,
- **enhance resilience by design**, through complete automation, fine-grained segmentation, and centralised governance,
- **keep control of data residency and governance**, in compliance with regulatory and sovereignty requirements,
- **reduce critical technological dependencies** by retaining control of infrastructures and architectures,
- **optimise resources and costs** by standardising environments and pooling strategic capabilities,
- **gradually modernise existing systems,** without interrupting operations.

OPCP is far more than an infrastructure tool; **it's a strategic foundation that helps OESs adapt, innovate, and secure their operations while staying aligned with their core mission.**

The following use cases clearly show how OPCP tackles tough, real-world problems faced by OESs in highly constrained and demanding environments.



OPCP

USE CASE | **01**

Modernising and securing an energy operator's IT systems

Modernising critical information systems while maintaining continuity and addressing cyber threats.

National energy operators rely on complex information systems, such as Supervisory Control and Data Acquisition or Operational Technology (SCADA/OT), network management, business applications, maintenance platforms, and analytics tools. Due to the energy transition and digital transformation of operations, data flows have significantly increased and the links between IT and OT have become stronger. In parallel, there has been a rise in attacks directed at the energy sector.
Previously separate systems are now interconnected and vulnerable, increasing operational risk.

With OPCP, they can:

- → **unify and secure infrastructure** IT and OT on a controlled foundation,
- → **strictly isolate critical** systems usin segmentation,
- → **locally host** data and sensitive applications,
- → **ensure business continuity**, even during a crisis or network outage,
- → **gradually modernise IT systems** without interrupting operations.

With OPCP, an energy operator can secure and update its IT systems, while ensuring operational continuity and national resilience.

OPCP

USE CASE | **02**

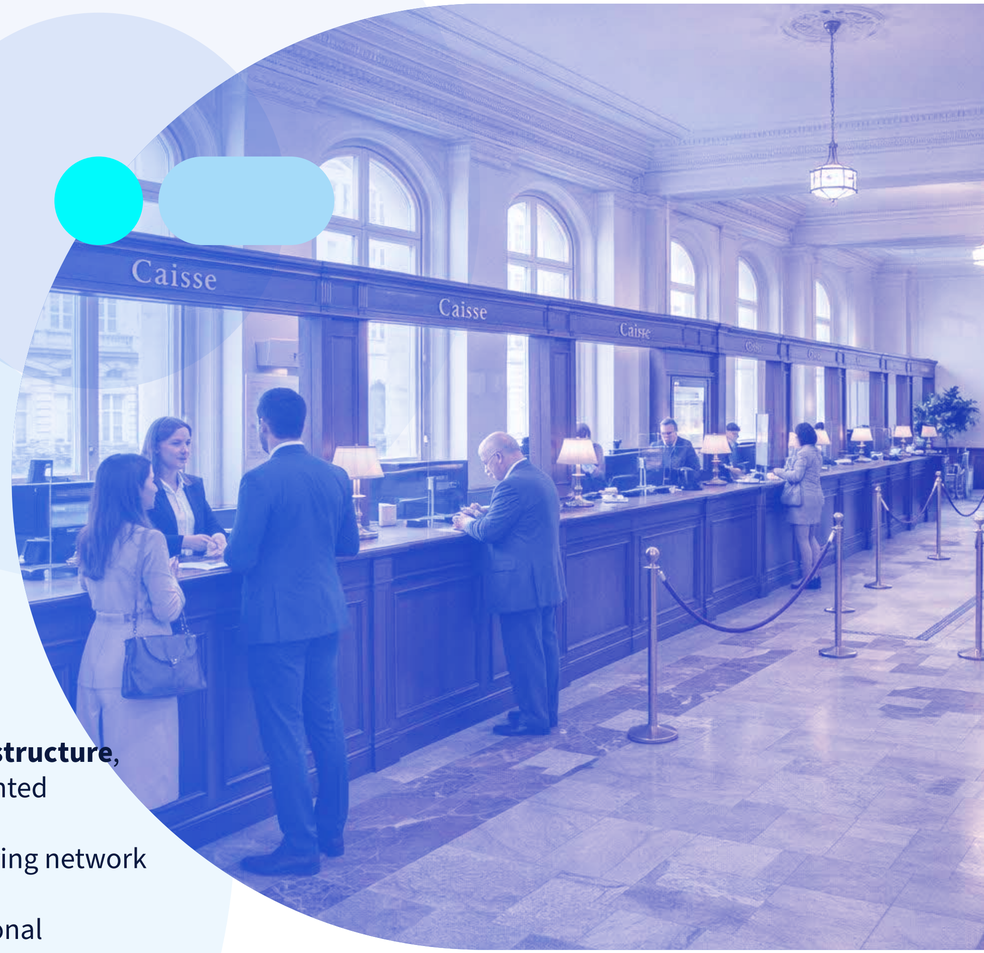
National payment system resilience

Ensuring financial stability and operations amid serious cyber threats.

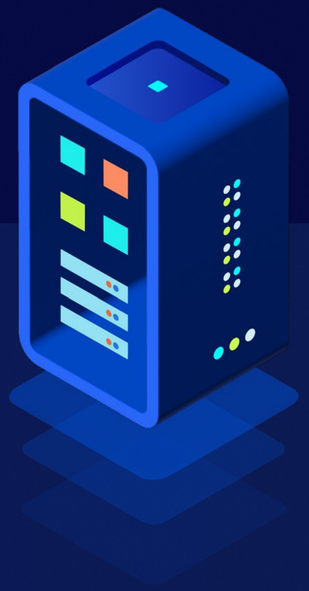
National interbank payment systems process massive transaction volumes in real time. An interruption, even briefly, could impact the national economy and shake market confidence. Cyber threats against financial institutions are on the rise, with a focus on disrupting services through denial of service attacks, or infiltrating essential systems.

With OPCP, they can:

- **deploy a resilient distributed infrastructure**,
- **isolate critical processing** in segmented environments,
- **maintain local capabilities** even during network outages,
- **ensure** complete access and operational **traceability**,
- **ensure faster recovery** after an incident.



OPCP improves the stability of financial systems through sovereign and controlled operational continuity.



OPCP

USE CASE | **03**

Securely managing a national water supply network

Ensuring continuous water supply and public health monitoring.

Water operators manage distributed infrastructures, including pumping stations, treatment plants, distribution networks, and integrated quality control systems. These facilities rely on sensors, industrial control systems, and interconnected monitoring platforms.

Any disruption, whether cyber or physical, can directly impact public health and social stability.

With OPCP, they can:

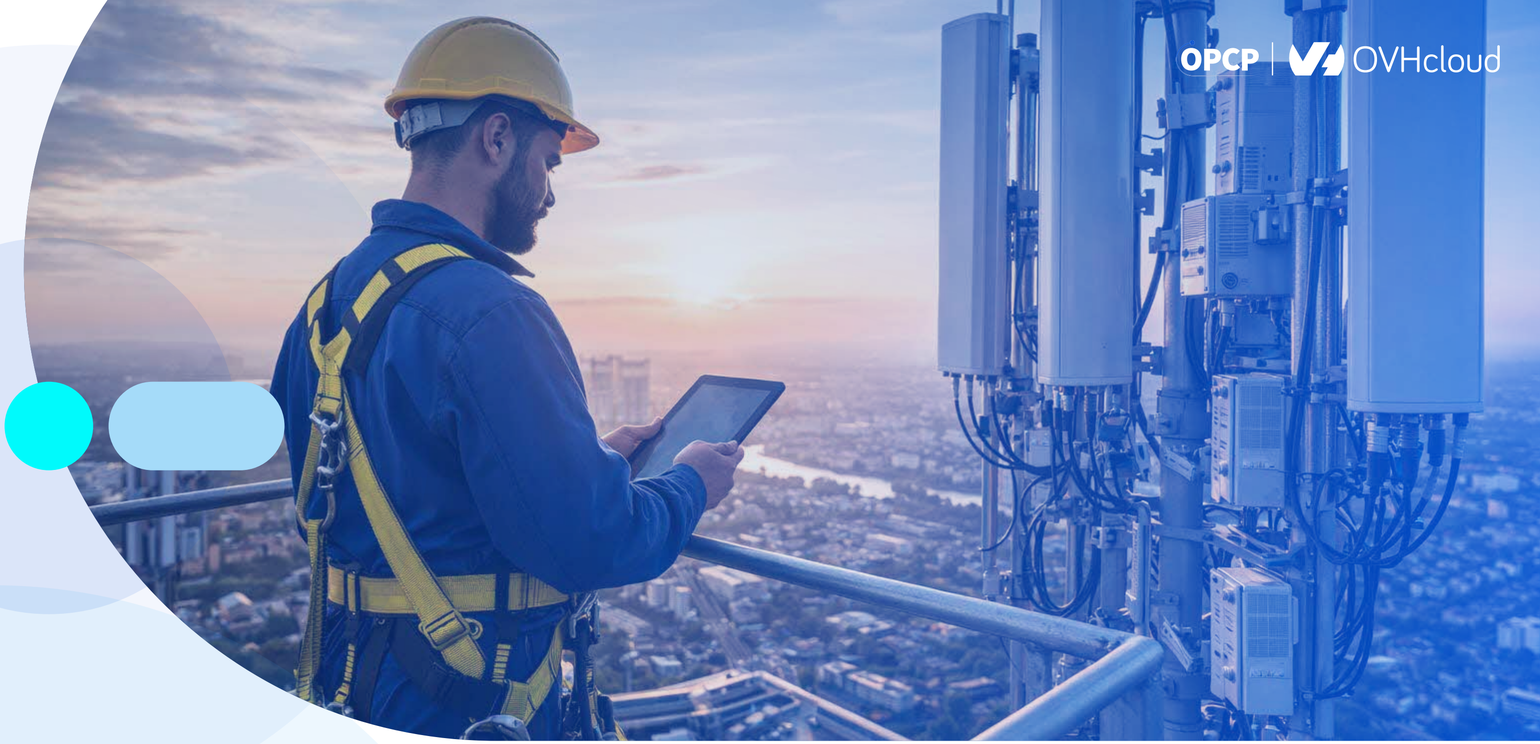
- **ensure the security of** industrial **monitoring systems**,
- **isolate** sensible **environments** by geographical area,
- **deploy edge capabilities** on remote sites,
- **analyse** water quality **data in real time** within a sovereign infrastructure,
- **guarantee operational continuity**, even with unreliable connectivity.

OPCP provides water distribution networks with a resilient foundation, ensuring public health safety and essential service continuity.

OPCP

USE CASE | **04**

Securing strategic telecom operators



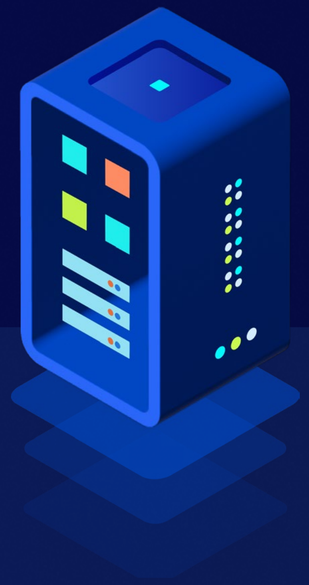
Maintaining the availability of national networks under pressure.

Today, national telecom operators are considered critical infrastructures — any downtime could disrupt emergency services, government operations, and the entire digital economy.
These environments are distributed, heterogeneous, and heavily utilised.

With OPCP, they can:

- **deploy** secure **edge capabilities** on regional nodes,
- **automate the management of** distributed **infrastructures**,
- **isolate sensitive environments,**
- **ensure** unified, centralised **monitoring**
- **maintain local operations**, even in isolated environments.

The ability of national telecom networks to withstand operational pressures can be strengthened using OPCP.



OPCP

USE CASE | **05**

Strategic industry and classified environments

Deploying advanced capabilities in an air-gapped setup.

Industries vital to national security and defence handle highly sensitive, classified information. Some infra-structures require total isolation — without an external connection — as well as modern capabilities (e.g., AI, simulation, HPC).

With OPCP, they can:

- → **deploy a** complete **infrastructure** in an air-gapped environment,
- → **pool advanced** local GPU or compute **resources**,
- → **ensure strict segmentation** by classification level,
- → **automate deployments** without external dependencies,
- → **maintain centralised governance** within an isolated setup.

OPCP provides a way to combine modern technological advancements with full sovereignty, especially where security is crucial.

OPCP

USE CASE | **06**

National rail system resilience

Maintaining the uninterrupted movement of people and goods.

National rail networks rely on signalling systems, traffic management, ticketing systems, and real-time monitoring. These environments are highly interconnected and distributed, with strict availability requirements. The modernisation of rail systems using advanced digital technologies (IoT, predictive maintenance, intelligent traffic management) increases exposure to cyber threats.

With OPCP, they can:

- **unify** control centre and regional site **infrastructures**,
- **strictly segment** critical signalling **systems**,
- **deploy edge capabilities** in key operational locations,
- **ensure high availability** across multiple sites,
- **update legacy applications** without disrupting operations.

Using OPCP, national rail systems can improve efficiency, safety, and resilience while maintaining public service continuity.

A pairing with purpose

A proven technical solution, combined with industry-specific expertise.
Clearly, there are things we need to do together.

Cases to develop, adapt, and test

There’s no shortage of use cases: edge, factories, critical sites, disconnected infrastructure, and much more. What if we focused on one or two key areas to make real progress?

A workshop, a chat, or a POC?

We don’t need to put everything on hold just yet. Let’s brainstorm, see which ideas make sense, and gradually build.

ovhcloud.com
opcp@ovhcloud.com