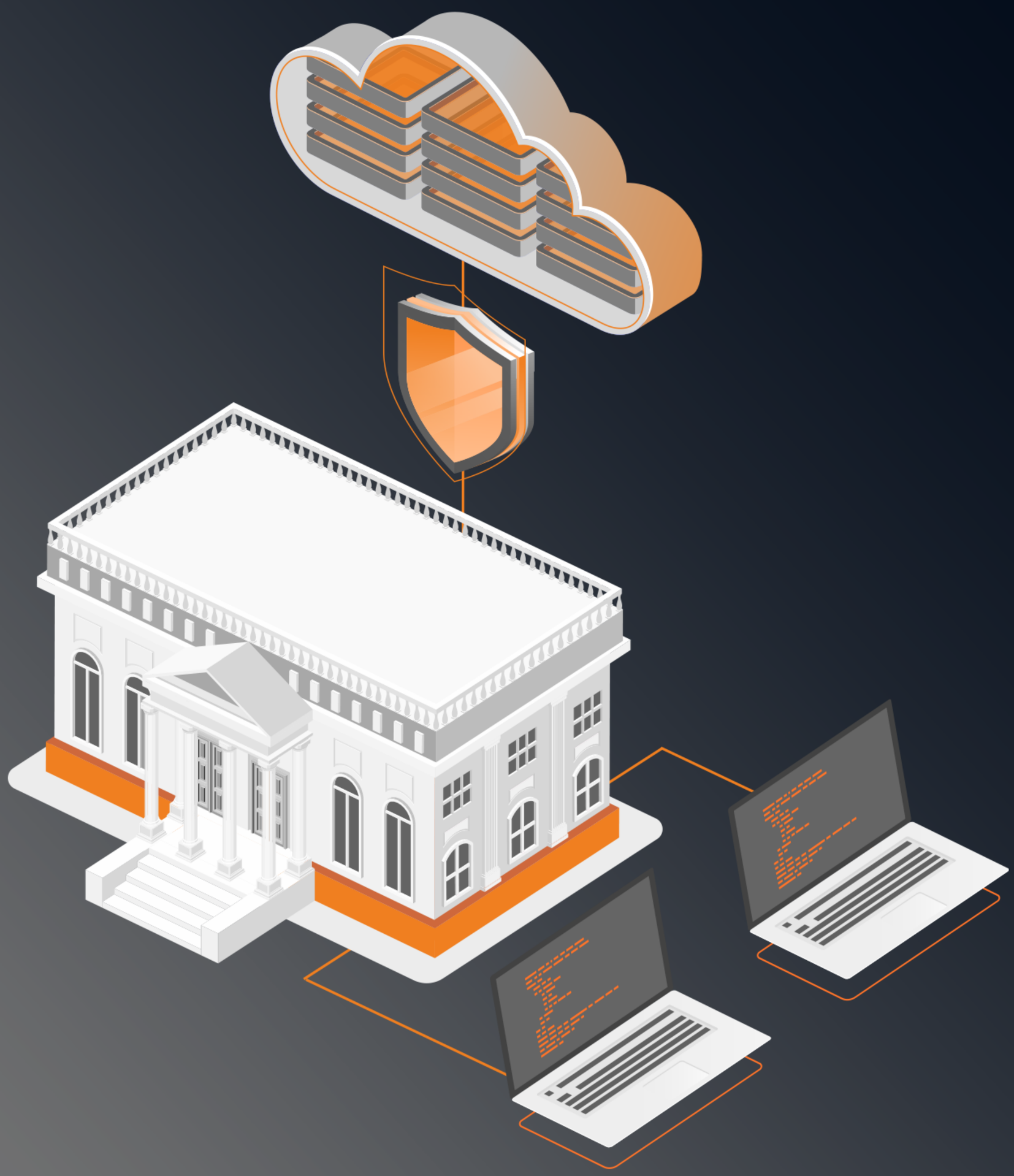
enclaive

Boosting the secure Digitalization within the Public Sector



www.enclaive.io

Confidential Containers in Action: Boosting the Digitalization within the Public Sector

Institutions around the world have seen a massive shift toward digital transformation within the last couple of years. And the pandemic has only accelerated the government's digital change efforts and sped up the pace of innovation. Public institutions are highly regulated sectors because of their valuable databases. Government agencies share a unique position when it comes to protecting data. Because they are responsible for safeguarding public safety and citizens' most sensitive information. This also means that the move to the cloud of a government agency is equivalent to high-risk processes with numerous vulnerabilities.

ENCLAIVE GMBH
WWW.ENCLAIVE.IO
CHAUSSE ESTR. 40
101 15 BERLIN

The Challenges

On-premise infrastructure is coupled with a high maintenance cost, low efficiency and agility, and limited scalability. Moreover, the public sector usually has little to no manpower or the necessary skills to uplevel its infrastructure. Especially for public institutions, it is impelling to embrace the efficiency of the public cloud, as these government agencies have a big data workload to operate with.

But before such a move can be considered, data security is the most intense concern for public agencies when moving vital workloads across the cloud. Data migration comes with high risks and numerous vulnerabilities, including incomplete data migration, corrupt or missing files, accidents, phishing, malware, or ransomware.

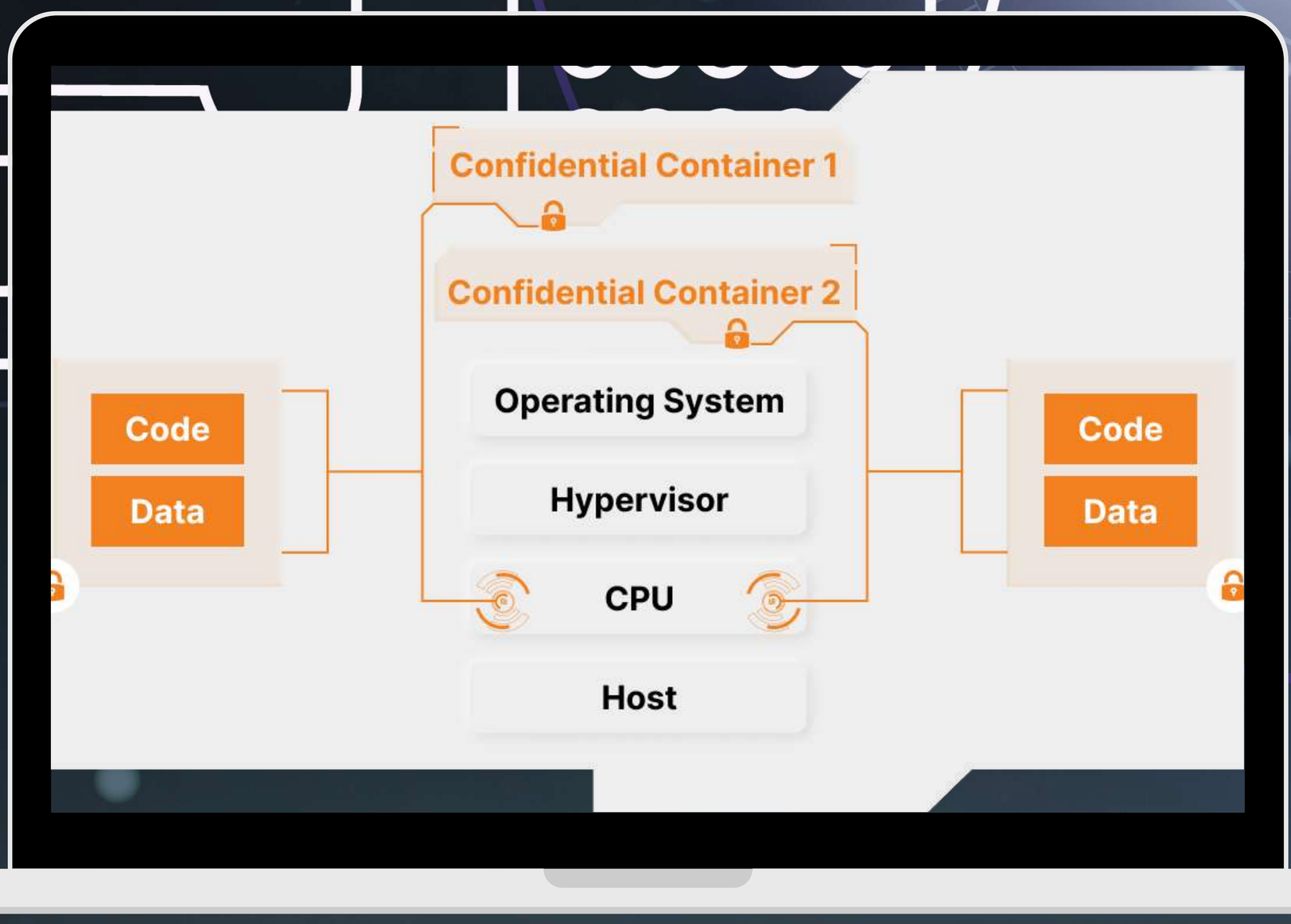
Summing up, the most notable concerns about data security focus on the following areas

- **How to prevent insider/outsider threats and third parties?**
- **How to ensure secure and untrusted collaboration with other institutions?**
- **How to prevent data breaches and ensure data privacy compliance?**

Solution Overview

In this context, the emerging technology of Confidential Computing can be used to secure citizens’ data, while also complying with data privacy regulations like GDPR. In a nutshell, confidential computing is a new computing paradigm safeguarding that citizens' data and sensitive data at any moment in time, while it is stored, looked up, edited or processed, remains encrypted and shielded against data breaches. Only legitimate users may access the data.

By design, our data stored in any government institution is given the safest harbour. Government institutions can turn their applications into confidential applications with ease thanks to enclaive’s revolutionary confidential container technology.



Enclaive’ Confidential Containers leverage the Confidential Compute Technology and are designed to protect both data and the application, even on untrusted infrastructure.
Throughout the data lifetime, sensitive data is always encrypted in memory and stays protected while being processed. Confidential computing technology ensures that **citizens' data stays anonymized**, while - say residents apply for a government service using their digital identity as online identification.

Furthermore, these confidential microservices would enable secure **cross-departmental collaboration and multi-party training of AI** for different purposes. The technology enables multi-party analytics in cases where the data owner might want to share a portion of a dataset while protecting the rest from view. Government institutions want to share sensitive information with, say, a financial institution. Until now, the option of sending it via email or saving it on a typical server would be coupled with high risks of data breaches. However, now each party could place the data in an encrypted enclave to allow secure access. Confidential Containers can therefore allow public institutions to share data bidirectionally without exposing it.

Enclaive **reduces the legal and IT-compliance efforts** by providing Confidential Container technology that meets GDPR regulations at all times. Hence, any attempt to hack this information is prevented by the privacy box, allowing for storing and processing data in a privacy-enhanced way. Moreover, the container may be attested at any point in time to the integrity and confidentiality of the code and data.

Further application scenarios

Let’s be practical, how can this technology benefit us, citizens? At the centre of all online activities operated by the administration are the **digital identity and the possibility of providing evidence of who is applying for the service**. Each contract agreement presumes that the contractual partners can identify themselves unequivocally and legally. Thus, a digital identity would ensure such an online identification. Such an eID function would be a major game-changer within the public service sector.
Users can move around the Internet safely and more freely by using this **so-called eID function**. This would pave the way for a whole package of citizen services or bank services that could be now operated online.

Use Cases for Online Citizen Services:

Issuing a new identity card

Applying for services from insurance companies

Requesting child care service online

Read enough? Click here to jump right in.

Why should you choose enclaive?

Give citizens' IT the safest place

Make Data Privacy a friend - not foe

Frictionless deployment

Be ready for Compliance Audits

Testimonials:

"Our fintech platform for the eHealth sector requires the highest security and privacy compliance, which we could implement at reduced costs with enclaive technology."
Martin Buhl, CEO cure digital finance GmbH

"In the transition of digitalizing the hospital IT (KHGZ) enclaive's technology helped us to implement many new IT projects with ease and in consensus with the data security officer."
Alexander Mommert, CEO Immanuel Klinik Rüdersdorf

Why should you choose enclaive?

Give citizens' data the safest place

Wrapping government IT with confidential containers means deploying the highest standard of security and privacy to protect sensitive data. It is so secure, that even the underlying infrastructure administrator may not access it.

Make Data Privacy a friend - not foe

By design, data while in use is fully encrypted. Only legitimate endpoints may access the data in cleartext. This way, Confidential Compute is a modern data anonymization technique, as no clear text data may be leaked.

Be ready for Compliance Audits

How can you prove that you have taken the best efforts to protect your IT? Running your IT shielded by confidential containers allows you to audit the containers and obtain a digital certificate that sensitive data runs in confidential containers.

Frictionless deployment

Our highly secure containers are built to work right out of the box. No changes to the application code or SDKs are required.

Want to know more?

Get in touch and let us walk you through a demonstration of how our Confidential Containers can boost the digitalization of your public institution.

>>> Watch a demo

>>> Try it out

If you want to get to know Enclaive:

>>> Product Portfolio

>>> In the Press

>>> About Us

EMAIL:
contact@enclaive.io

WEB:
enclaive.io