SOLUTION BRIEF

CYSEC AND SYNTHETICUS

Turn data from a liability into an asset with Synthetic Data and Confidential Computing

CYSEC, an operating system provider leveraging Confidential Computing, and Syntheticus, a software provider for synthetic data, have announced a strategic global partnership to empower businesses to extract the maximum value of their sensitive data in a privacy preserving way

These days, corporate data is growing in number and increasingly recognized as having business value.
According to the Gartner Chief Data Officer Survey, data and analytics leaders who share their data externally generate 3x more measurable economic benefits than those who don't. Organizations that provide access to internally and externally prepared data realize 2x the business value of analytics investments than those who don't, and D&A leaders who promote data sharing have more stakeholder engagement and influence than those who don't.

In addition, cloud solution providers (CSPs) offer the most effective data analytics tools, such as Google Analytics, to extract value from data within organizations.
However, organizations must comply with data protection and privacy regulations that limit access to these tools.

The Cysec-Syntheticus strategic global partnership brings together deep skills in advanced Privacy-Enhancing Technologies marrying cutting-edge AI with state-of-the-art cryptography as well as profound know-how on product integration to help support clients through successful digital transformations.

CONTACT

CYSEC - Matthieu Legré
VP Product Manager
matthieu.legre@cysec.com

SYNTHETICUS - Aldo Lamberti
CEO & Founder
aldo.lamberti@syntheticus.ai

GOVERNMENTAL REGULATIONS CONTEXT

- The Court of Justice of the European Union (CJEU), in its July 16 2020 ruling, invalidated the Privacy Shield, a mechanism that framed personal data transfers between the European Union and the United States.
- The U.S. legislation does not offer sufficient guarantees against the risk of access by authorities, including intelligence services, to the personal data of European residents
- The Italian privacy authority, the Garante, deemed that the use of Google Analytics results in unlawful transfers of personal data to the United States in violation of the principles outlined in the Schrems II ruling.

Aligning with positions already expressed by privacy regulators in Austria and France, the Garante has taken a clear stance on the compliance of data transfers to the United States made through Google Analytics, ordering the website provider to suspend its use if it does not comply with the Garante's requests.

ANALYSIS

Current state of sensitive data analysis in public clouds through two options

OPTION 1 - Status quo

Organizations tend to keep their own sensitive and valuable data in secure data centers. In this case, they need to deploy and operate their own analytic tools or the ones of a third party. This solution has the disadvantage not to benefit from the cost reduction and the elasticity provided by running CSP solutions in cloud environments.

OPTION 2 - Investigation on the use of privacy enhancing technologies (PET) to isolate their own data from CSP.

One PET called 'Synthetic Data' allows the end-user to exploit CSP data analytics tools without revealing the exact value of its data. The European Data Protection Supervisor defines synthetic data generation as "to take an original data source (dataset) and create new, artificial data, with similar statistical properties from it". When the original data set size is large, the generation of synthetic data requires a large amount of resources and thus the cloud is the ideal place to compute on. The drawback is in this case that the original data set can be accessed by CSP.

Another PET called 'Confidential Computing' exploits hardware-based Trusted Execution Environments (TEEs) in processors. These TEEs cryptographically isolate the code and data executed in the cloud from the CSP host OS and CSP hypervisor. The drawback is in this case that CSP analytic tools can't be used without breaking the isolation between data and the CSP admins.

CHALLENGE

Is it possible for organizations to leverage the power of CSP analytics tools while strictly blocking the CSP from accessing and extracting value from their own data?

Cysec and Syntheticus partner up for a joint solution of privacy preserving synthetic data in cloud environments through Confidential Computing. Indeedboth PET's, synthetic data and confidential computing, complement each other to implement use-cases where data privacy is preserved inclouds while leveraging powerful CSP analytic tools.

CYSEC

Syntheticus

Let's see this solution integrated in 2 use-cases.

USE-CASE #1

Extend your on-prem IT infrastructure with powerful CSP tools through privacy-preserving synthetic data

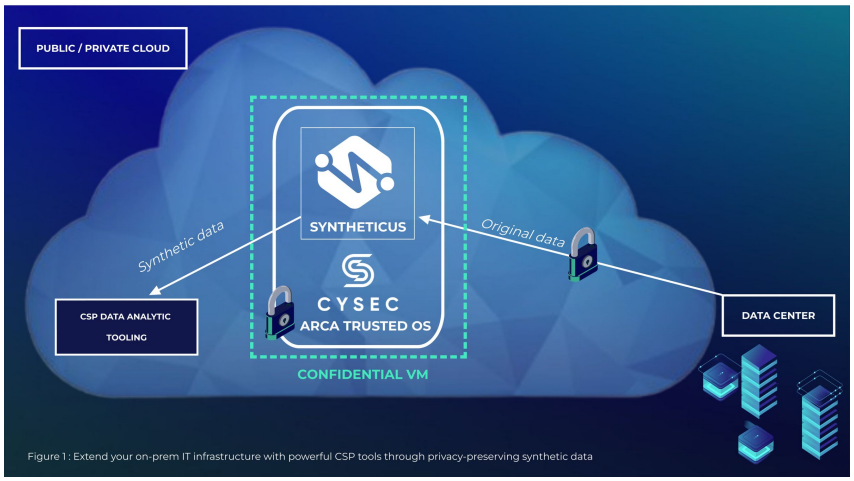


Figure 1 : Extend your on-prem IT infrastructure with powerful CSP tools through privacy-preserving synthetic data

The end-user has its entire IT infrastructure that runs on-premises. Nevertheless the end-user needs to exploit CSP analytic tools to extract value from its data.

One way to go is to use synthetic data instead of the original sensitive data. However, the generation of synthetic data requires costly local infrastructure that might be used only occasionally.

The solution is to deploy Syntheticus within isolated ARCA Trusted OS instances in clouds powered by confidential computing.

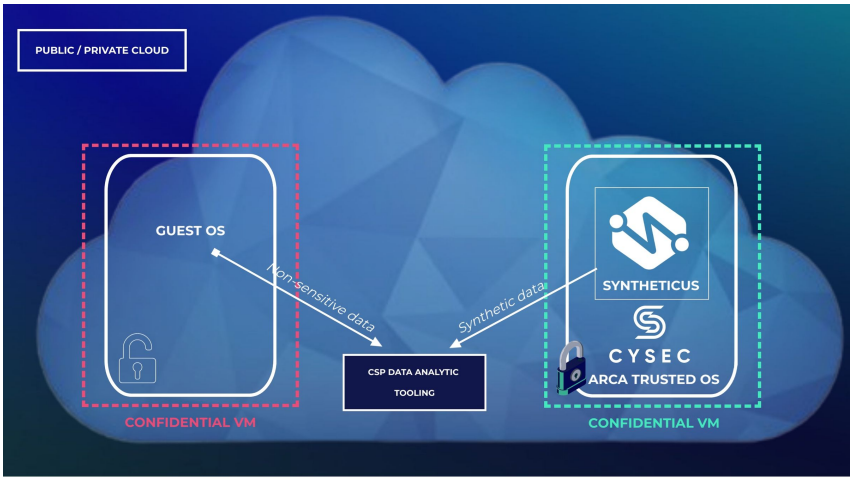
How does it work?

1. The sensitive data is securely sent from the Data Center to Syntheticus synthetic data generator located in the cloud and isolated from the CSP thanks to the combination of ARCA Trusted OS with a hardware-based TEE.
2. The synthetic data is generated in the isolated cloud instances.
3. Then, the synthetic data can be analyzed with powerful CSP data analytic tooling without compromising sensitive data privacy.
4. Ultimately, the original sensitive data is securely deleted in the isolated cloud instances.

VALUE : You extend the capabilities of your on-prem IT infrastructure with powerful CSP data analytic tools with the help of privacy-preserving synthetic data to extract the maximum value of data.

USE-CASE #2

Leverage privacy-preserving synthetic data to benefit from powerful CSP tools without breaking isolation provided by confidential computing



The end-user has migrated sensitive data and processes in clouds benefiting from the isolation offered by ARCA Trusted OS deployed in VMs running in a confidential computing context. The end-user IT infrastructure in clouds might be composed of two types of instances: some conventional instances operating non-sensitive processes handling non-sensitive data that can be exposed to CSP admins, and some isolated instances operating sensitive processes handling sensitive data that cannot be exposed to CSP admins. This type of cloud migration strategy allows the use of CSP data analytic tools on non-sensitive data, but prevents the use of the same tools on sensitive data

The solution is to generate synthetic data with Syntheticus within confidential VMs to allow the end-user to exploit CSP analytics tools, while the sensitive data is kept confidential in the isolated cloud instances.

How does it work?

1. Syntheticus is deployed in isolated ARCA Trusted OS instances, i.e Confidential VM running ARCA Trusted OS as guest OS, to allow the generation of synthetic data.
2. Then, the synthetic data is analyzed with powerful CSP data analytic tooling without compromising sensitive data privacy.

VALUE : You benefit from powerful CSP analytic tools to extract the maximum data value without breaking the isolation between your migrated cloud data and the CSP.

Conclusion

The joint solution proposed by Syntheticus and Cysec brings new opportunities of extracting value from data. This solution is addressed to organizations that cannot benefit from secure access to the powerful CSP analytics tooling either because they made the choice to keep their entire IT infrastructure on-premise or in confidential VMs in clouds. The joint solution enables this access while ensuring data privacy by combining two privacy enhancing technologies: Synthetic Data and Confidential Computing.

WHO WE ARE

About SYNTHETICUS

Syntheticus

Founded in 2021, Syntheticus is a fast-growing company headquartered in Switzerland providing B2B software solutions. Trusted by Microsoft, Nvidia, ETH AI Center and IMD. Backed by the prestigious Hammerteam Growth Accelerator and Schaffhausen Institute of Technology.

SYNTHETICUS' flagship solution, called Syntheticus Hub, is a synthetic data platform which empowers customers to turn sensitive data from a liability into an asset by enabling them to share & monetize data and ML models in a privacy preserving way. Syntheticus Hub
leverages advanced privacy enhancing technologies such as Generative AI and Differential Privacy, orchestrates multi-type data, provides seamless integrations with existing systems and maintains strong enterprise-grade data protection.

Further information can be found at www.syntheticus.ai or hello@syntheticus.ai

About CYSEC

CYSEC

CYSEC is a European data security company, based in Lausanne and Paris, providing a software solution in Confidential Computing, which enables companies to secure workloads on distributed infrastructures. The company provides a Trusted Execution Environment for containers and helps them to secure and deploy sensitive data on distributed architecture from Data center to the Cloud to the Edge.

CYSEC's flagship solution, called «ARCA Trusted OS» is a hardened Linux-based operating system combined with a secure Kubernetes orchestrator providing a trusted runtime platform for containers. ARCA provides cryptographic functions, in order to protect keys, code and data, be it at rest, in transit and in use.

Further information can be found at www.cysec.com or info@cysec.com