decentriq case study

Confidential computing solution built on Microsoft Azure fosters data ecosystems by protecting data at rest, in transit, and in use

Familiar obstacles hinder collaborative data ecosystems

Data ecosystems are valuable assets, but the process of creating collaborative data ecosystems is impeded by regulatory difficulties, complicated processes, and risk.

Confidential computing built on Microsoft Azure infrastructure

decentriq's solution, which uses Microsoft Azure virtualization infrastructure for confidential computing, enables data analysis without compromising security.

Accessing sensitive data without seeing the underlying assets

With decentriq's Confidential Query, enterprises can protect data at all stages of analysis, allowing for greater control over access and privacy.

Microsoft

A Microsoft partner specializing in privacy-assured computing environments

decentriq, a tech startup based in Zurich, Switzerland, is a leading company in the area of confidential computing. Together with Microsoft and Intel, decentriq is a founding member of the Confidential Computing Consortium, an alliance to accelerate the adoption of trusted execution environment (TEE) technologies and standards. A TEE uses a container to secure a portion of the hardware's processor and memory, protecting the code and data inside.

decentriq is changing the way enterprise customers create data ecosystems and analyze data with their partners by providing a secure and privacy-assured computing environment. In the process of stepping out of the lab and bringing its products to market, decentriq has engaged in proof-of-concept projects and collaborations with insurance, finance, pharmaceutical, and retail enterprises.

How Confidential Query protects data

decentriq's flagship product, Confidential Query, is available in the Microsoft Azure Marketplace. Confidential Query uses DCsv2-Series virtual machines for confidential computing infrastructure. These Azure virtual machines are designed to protect the confidentiality and integrity of data and code while it's processed in the cloud.

Confidential Query uses an SQL framework that is by design private. It enables enterprises to run any query using that framework, and it guarantees privacy-preserving results with zero chance of data leakage. These functions can help businesses achieve high trust, access unique insights, and remain compliant. They also give customers the opportunity to share and collaborate on sensitive datasets, including the ability to run analytics on them utilizing data models from different sources. The data and the model remain private, and invisible even to decentriq. Analysts and data scientists can run queries on confidential data without being able to see the underlying data assets. And through Python APIs or a web application, Confidential Query can integrate seamlessly into existing workflows without any code change.

By committing to the deployment of the technology, decentriq customers ensure data is protected at all stages of data analysis, keeping it safe at rest, in transit, and in use. decentriq has been able to extend and mature its product offering thanks to the flexibility and scalability of Azure. Deployment times have decreased and the opportunities to collaborate and partner with companies that also utilize cloud infrastructure have been simplified. Azure provides decentriq the advantage of fast and easy integrations, which allows customers to adopt, deploy, and gain value from its products without interrupting their workflows.

"For enterprises, initiating and participating in data ecosystems is a cumbersome process. Accessing, sharing, and analyzing sensitive data with external parties are non-trivial challenges. At decentriq, we facilitate this for our clients via our software platform using Microsoft Azure confidential computing. And with the Microsoft Azure Marketplace, we are able to make it more accessible."

- Maximilian Groth, CEO, decentriq