Privacy computing: why the best time to invest in the security and privacy of data in use is now

Privacy computing is an emerging technology that ensures data privacy and security while the data is being processed or used. In the current digital age, the amount of data being generated and processed is increasing exponentially. The need for privacy computing solutions is becoming more crucial than ever to ensure that sensitive information is protected from unauthorised access or misuse

Temps de lecture : minute

21 April 2023

The growing need for privacy computing

With the increase in data breaches, cyberattacks, and the use of personal data by various entities, there is a growing need to ensure the privacy and security of data. Privacy computing offers a solution to this problem by providing a secure environment where data can be processed without the risk of unauthorized access. It provides end-to-end encryption, ensuring that data is protected from the point of creation to the point of use. This makes it impossible for anyone to access or intercept data during processing, making it an ideal solution for businesses and individuals who handle sensitive data.

The benefits of investing in privacy

computing

Investing in privacy computing has several benefits. First, it ensures data privacy and security, which is crucial for businesses and individuals who handle sensitive information. This protects them from data breaches, cyberattacks, and other forms of unauthorized access. Second, it helps to build trust between businesses and customers, as customers are more likely to trust a business that prioritizes their privacy and security. Third, it helps businesses to comply with data protection regulations, such as the GDPR and CCPA, which require them to protect customer data. One of Decision3’s use cases that we cover is multi-party data collaboration. An example would be a university research group working on early disease detection AI, that needs to access patients' data from hospitals to train and test their models. Using our tech, we can deploy a trusted execution environment on the cloud, which enables such collaboration while ensuring full privacy of the data. We can also deploy the TEEs (trusted execution environment) within the hospital's network to ensure the data never leaves the premises.

It is crucial to remember that confidential computing enables companies to generate a lot of value from the data they already have. It does not only protect data that is already idling, but allows you to analyze it, train AI and ML models, make predictions, etc., while fully preserving the privacy and security of such data. Also, a huge technological breakthrough will be the ability to share data with other companies, while not violating the privacy of the data itself. Imagine a scenario where there's a big bank that's full of its customer data and can't do anything with it, and there's a fintech startup that needs that data to train its models/algorithms. Now this problem is not solved in any way. With the use of confidential computing, these participants will be able to collaborate on this data, while fully maintaining privacy and data security.

The risks of not investing in privacy computing

The risks of not investing in privacy computing are significant. Businesses that do not prioritize data privacy and security risk losing customer trust and damaging their reputation. They may also face legal consequences for failing to comply with data protection regulations. However, the greater risk is that they will not be able to do anything with this data. Companies that are currently investing in confidential computing will soon have an unfair advantage in their markets because with the development of AI and ML, their products and services will become better and better because their data will be a crucial resource that brings them value. Companies that do not invest in confidential computing will look at this data and have no idea what to do with it because they do not have a secure enough and privacy-preserving way to analyze and process such data.

Conclusion: Invest in Privacy Computing Now

In conclusion, privacy computing is an essential technology that businesses and individuals should invest in to ensure the privacy and security of data in use. The growing need for data privacy and security, coupled with the benefits of investing in privacy computing, makes it an ideal solution for businesses and individuals who handle sensitive data. The risks of not investing in privacy computing are significant, and businesses should take proactive measures to protect themselves and their customers. Therefore, investing in privacy computing now is the best course of action to ensure data privacy and security. Right now, the biggest challenge with confidential computing adoption is the necessity to modify your application to run inside trusted execution environments. Adoption of confidential computing will be greatly accelerated when it's possible to run unmodified applications in trusted execution environments while being protected by confidential computing Enclaves, providing quick time to value.

Currently, AWS Nitro is the closest in solving the problem, with all other major cloud providers investing significantly in their own confidential computing cloud products. The technology is definitely new and is hard to adopt. TEEs run independently of your OS and thus you have to refactor the code you have to be compatible with the TEEs that you are using. However, overall, privacy computing provides a solution to the growing need for data privacy and security. Investing in privacy computing has several benefits, including protecting sensitive information, building customer trust, and complying with data protection regulations. On the other hand, the risks of not investing in privacy computing are significant, including losing customer trust, damaging reputation, and facing legal consequences. Therefore, it is crucial for businesses and individuals to invest in privacy computing now to ensure data privacy and security.

Oleksandr Pukhalskyi is cofounder of *Decision3*.

Article by Oleksandr Pukhalskyi