

Google Cloud announces enhanced Confidential Computing

17 July 2020, by Peter Grad



Credit: Pixabay/CC0 Public Domain

Amid ever-increasing demands for privacy and security for highly sensitive data stored in the cloud, Google Cloud announced this week the creation of Confidential Computing.

Terming it a "[breakthrough technology](#)," Google said the technology, which will offer a number of products in the coming months, allows users to encrypt [sensitive data](#) not only as it is stored or sent to the cloud, but while it is being worked on as well.

Confidential Computing keeps data encrypted as it's being "used, indexed, queried, or trained on" in memory and "elsewhere outside the central processing unit," Google said in a statement about the new technology.

The first product, Confidential Virtual Machines, was formally announced at Google's annual Cloud Next conference being held online this year, due to COVID-19 restrictions, over a nine-week period. It builds upon its Google Cloud Services unveiled by Google and AMD earlier this year that featured processors capable of generating and managing

[encryption keys](#) that remain on the chip.

Google said Confidential Computing is a step beyond isolation and sand-boxing currently employed on virtual machines.

"Confidential VMs take this to the next level by offering memory encryption so that you can further isolate your workloads in the cloud," Google said in an online statement announcing the technology.

Google is using AMD's Secure Encrypted Virtualization feature of its massive second-generation EPYC processors. These allow demanding processing tasks to proceed with real-time encryption by dedicated VM instance keys generated by and residing solely within the VM. This approach blocks access by Google and other VMs running on the host site, and the encryption keys cannot be exported.

The program will not compromise current performance. And because no coding is required, the transition to the bolstered platform will be seamless. Confidential Virtual Machines, in fact, can be accessed by clicking a single checkbox.

Google said the program is not simply an add-on feature but is an integral component covering the entire Google Cloud Platform.

"We believe this is a foundational differentiator for Google Cloud in these regulated markets," Google Cloud General Manager Sunil Potti said. Describing Confidential Technology as "game-changing technology," Potti referred to companies that had withheld their most sensitive data from the cloud due to security concerns: "It's almost like the last bastion of sensitive data that can now be unlocked to leverage the full power of the cloud."

AMD's Greg Gibby explained the advantage of enhanced security provided by [virtual machines](#) under Google Cloud Services in an interview with Wired magazine.

"If I look at today, an admin has the ability to peer in and see what's going on in each one of those VMs. And if I have a bad actor on one of those VMs there are tools that they can use to break out into neighbors' VMs, peer inside and see the data, because it's all unencrypted," Gibby, a senior product manager, said. "But now, as the admin spins up VMs, they can no longer peer into those VMs and see the data. And if I have a bad actor in those VMs and they break into another one, they can't see the data that's encrypted."

Google joins several other major players aiming to make cloud computing more secure. Microsoft and IBM expanded access to more secure virtual machine environments earlier this year.

More information:

cloud.google.com/confidential-computing

© 2020 Science X Network

APA citation: Google Cloud announces enhanced Confidential Computing (2020, July 17) retrieved 1 December 2021 from <https://techxplore.com/news/2020-07-google-cloud-confidential.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.