July 14, 2020

Advanced Security Features of AMD EPYC™ Processors Enable New Google Cloud Confidential Computing Portfolio

AMD Secure Encrypted Virtualization feature enables breakthrough Confidential VM offering from Google Cloud

SANTA CLARA, Calif., July 14, 2020 (GLOBE NEWSWIRE) -- AMD (NASDAQ: AMD) and Google Cloud today announced the beta availability of Confidential Virtual Machines (VMs) for Google Compute Engine powered by 2nd Gen AMD EPYC™ processors, taking advantage of the processors' advanced security features.

The first product in the Google Cloud Confidential Computing portfolio, Confidential VMs, enables customers for the first time to encrypt data in-use while it is being processed and not just when at rest and in-transit. Based on the N2D family of VMs for Google Compute Engine, Confidential VMs provide customers high performance processing for the most demanding computational tasks and enable encryption for even the most sensitive data in the cloud while it is being processed.

"At Google Cloud, we believe the future of cloud computing will increasingly shift to private, encrypted services where users can be confident that the confidentiality of their data is always under their control. To help customers in making that transition, we've created Confidential VMs, the first product in our Google Cloud Confidential Computing portfolio," said Vint Cerf, vice president and chief internet evangelist, Google. "By using advanced security technology in the AMD EPYC processors, we've created a breakthrough technology that allows customers to encrypt their data in the cloud while it's being processed and unlock computing scenarios that had previously not been possible."

"As enterprises migrate tasks to the cloud for reasons including ease of management, scalability, and reduced costs, they often stop short of moving more sensitive workloads due to security concerns," said Dan McNamara, senior vice president and general manager, Server Business Unit, AMD. "To help provide the confidence that customers can move their sensitive workloads to the cloud, AMD and Google worked together on the Google Confidential VMs to take advantage of an advanced security feature, Secure Encrypted Virtualization, within AMD EPYC processors. This helps enable a unified and consistent level of hardware-based security for applications and workloads in the cloud. As well, AMD and Google have worked together to help customers both secure their data and achieve high performance of their workloads."

The Confidential VMs from Google provide:

- **Real time encryption-in-use** – Google Cloud customers can encrypt data-in-use, taking advantage of advanced security features offered by the 2nd Gen AMD EPYC

processor together with Confidential Computing cloud services, bringing a breakthrough in the level of cloud data protection,
- **Secure Encrypted Virtualization (SEV) –** an advanced security feature available on AMD EPYC processors, which encrypts VM memory using a dedicated per-VM key that is generated and managed by the embedded security processor,
- **"Lift and Shift Confidentiality" –** AMD and Google have simplified the use of Confidential Computing, making the transition to Confidential VMs seamless as customers do not need to make any code changes to their applications to benefit from these VMs,
- **High-performance VMs** – Confidential VMs offer similar performance to Google N2D VMs, which are powered by high-performance 2nd Gen AMD EPYC processors.

Driving Innovation with AMD and Google

Confidential Computing can unlock computing scenarios previously not possible, including:

- Multi-party Computation – Situations in which organizations want to collaborate with each other on private datasets, while protecting the confidentiality of the data.
- Data Access and Confidentiality – Confidential VMs can limit the exposure of the data and who can access it by encrypting the data even when it is being processed.

Organizations will be able to share confidential data sets and collaborate on research in the cloud across geographies and competitors confidently due to the high-performance capabilities and advanced security features of the AMD EPYC processors coupled with the innovative Confidential Computing technology offered by Google.

AMD EPYC Processors, Powering the Modern Security Focused Cloud

AMD EPYC processors power more than 120 VM types from cloud providers and hosts around the world that support a variety of workloads including high-performance, general purpose, memory bound and more.

As well, AMD is committed to supporting the advancement for security across cloud computing as it recently joined the Confidential Computing Consortium.

Confidential VMs are available to all GCP customers in the following GCP regions - asia-southeast1, europe-west1, europe-west4, us-central1 and are available for Google Compute Engine in Beta.

Supporting Resources

- Read more about Confidential VMs at the Google Cloud blog here
- Learn more about AMD EPYC processors here
- Learn more about AMD EPYC for the cloud here
- For workload solutions by AMD for the confidential VMs, visit here
- Follow AMD on Twitter

About AMD

For more than 50 years AMD has driven innovation in high-performance computing, graphics and visualization technologies — the building blocks for gaming, immersive platforms and the datacenter. Hundreds of millions of consumers, leading Fortune 500 businesses and cutting-edge scientific research facilities around the world rely on AMD technology daily to improve how they live, work and play. AMD employees around the world are focused on building great products that push the boundaries of what is possible. For more information about how AMD is enabling today and inspiring tomorrow, visit the AMD (NASDAQ: AMD) website, blog, Facebook and Twitter pages.

AMD, the AMD Arrow logo, EPYC and combinations thereof, are trademarks of Advanced Micro Devices, Inc. Other names are for informational purposes only and may be trademarks of their respective owners.

Contact:
Aaron Grabein
AMD Communications
(512) 602-8950
aaron.grabein@amd.com

Laura Graves
AMD Investor Relations
(408) 749-5467
laura.graves@amd.com



Source: Advanced Micro Devices