Google Cloud Announces New Capabilities to Simplify Security Operations and Strengthen Data Protection

Confidential VMs and Assured Workloads for Government provide customers advanced security tools to support compliance and data confidentiality

Sunnyvale, CA, July 14, 2020 — Google Cloud today announced two new security offerings,Confidential VMs, the first product in its Confidential Computing portfolio, and Assured Workloads for Government. Both underscore Google Cloud's commitment to serving customers in highly regulated and security-sensitive industries, such as the public sector, healthcare, and financial services.

More than ever before, enterprises are balancing the need to reduce complexity and cut costs while maintaining security and compliance. This includes meeting audit and regulatory requirements, making sure only the right people have access to sensitive data, and evolving their digital strategies to stay ahead of emerging threats.

Google has been operating securely in the cloud for more than 20 years. Leveraging its reliable, global infrastructure and trailblazing security innovations like BeyondCorp's zero trust access model, Google Cloud is able to deliver unique capabilities that require minimal operational overhead. Customers do not need to choose between ease of use and advanced security, so their teams can focus on important tasks at hand like emerging cyber threats.

"Customers across all industries are navigating the complexities of compliance and privacy in the cloud, especially those in regulated industries, such as financial services firms, healthcare companies, and government agencies," said Sunil Potti, General Manager and VP of Security at Google Cloud. "These companies want to adopt the latest cloud technologies, but strict requirements for data privacy or compliance are often barriers. Confidential VMs and Assured Workloads will help us better serve customers in these industries, so they can securely take advantage of the innovation of the cloud while also simplifying security operations."

Enabling new possibilities in the cloud with Confidential Computing

As organizations move workloads to the cloud, one of the biggest concerns they have is how to process sensitive data while keeping it private. Google Cloud encrypts data at-rest and in-transit, but customer data must be decrypted for processing. Confidential Computing is a breakthrough technology which encrypts data in-use -- while it is being processed. Confidential Computing environments keep data encrypted in memory and elsewhere outside the central processing unit (CPU). This technology will transform the way organizations process data in the cloud, maintain control over their data, and preserve confidentiality.

"Rarely do new technologies emerge that can fundamentally change the nature of cloud computing," said Vint Cerf, Chief Internet Evangelist at Google. "Confidential Computing is one of those game changers that has the potential to transform the way organizations process data in the cloud, while significantly improving confidentiality and privacy."

Confidential VMs is the first product in Google Cloud's Confidential Computing portfolio. Google Cloud already employs a variety of isolation and sandboxing techniques as part of its cloud infrastructure to help make its multi-tenant architecture secure. Confidential VMs takes this to the next level by offering memory encryption so that customers can further isolate workloads in the cloud. Google Cloud is the first major cloud provider to offer this level of security and isolation while giving customers an easy-to-use solution that doesn't require changing code in apps or compromising performance. Confidential VMs is available on AMD EPYC™ CPUs and takes advantage of the Secure Encrypted Virtualization (SEV) feature supported by 2nd Gen AMD EPYC CPUs.

"Our deep partnership with Google Cloud on its Confidential VMs solution helps ensure that customers can secure their data and achieve performance when adopting this transformational technology," said Dan McNamara, Senior Vice President and General Manager, Server Business Unit, AMD. "Confidential VMs offer high performance for the most demanding computational tasks all while keeping VM memory encrypted with a dedicated per-VM instance key that is generated and managed by our hardware."

Confidential Computing can unlock computing scenarios that had previously not been possible. Organizations will be able to collaborate in the cloud, all while preserving the confidentiality of their data.

Compliance without compromise through Assured Workloads

For government agencies that want to modernize IT with cloud technologies, ensuring the security, privacy, and regulatory

compliance of their workloads is imperative. To address this, many cloud providers have built separate environments (also known as “government clouds”) to meet the strict compliance requirements for processing government data. This results in government agencies having to run on less feature-rich, fortressed versions of commercial clouds to meet their needs.

Google Cloud believes there is a better way, and today is introducing Assured Workloads for Government, which offers customers the ability to easily and quickly create controlled environments in which U.S. data location and personnel access controls are automatically enforced. Assured Workloads for Government enables federal, state, and local agencies to serve critical workloads that leverage the latest cloud capabilities, without compromising on compliance.

Confidential VMs is currently in Beta. Assured Workloads for Government is currently in Private Beta in US regions, and will be made generally available (with Beta features) in the fall. For additional information, please see our blogs on Confidential VMs and Assured Workloads.

About Google Cloud

Google Cloud provides organizations with leading infrastructure, platform capabilities, and industry solutions. We deliver enterprise-grade cloud solutions that leverage Google’s cutting-edge technology to help companies operate more efficiently and adapt to changing needs, giving customers a foundation for the future. Customers in more than 150 countries turn to Google Cloud as their trusted partner to solve their most critical business problems.

AMD, the AMD Arrow logo, EPYC and combinations thereof are trademarks of Advanced Micro Devices, Inc.

---

https://www.googlecloudpresscorner.com/2020-07-14-Google-Cloud-Announces-New-Capabilities-to-Simplify-Security-Operations-and-Strengthen-Data-Protection