Confidential VMs

Ensure confidentiality of your most sensitive data in the cloud—even while it's being processed. Confidential VMs is now in BETA.

At Google, we believe the future of cloud computing will increasingly shift to private, encrypted services that give users confidence that they are always in control over the confidentiality of their data. While there are existing technologies that protect data by encrypting it in transit and at rest, confidential computing encrypts data in-use, while it's being processed. Confidential VMs is the first product in Google Cloud's Confidential Computing portfolio. Confidential VMs offer memory encryption so that customers can isolate workloads in the cloud.

Breakthrough confidentiality

Customers can now protect the confidentiality of their most sensitive data in the cloud even while it's being processed. Confidential VMs leverage the Secure Encrypted Virtualization (SEV) feature of 2nd Gen AMD EPYC™ CPUs. Your data will stay encrypted while it is used, indexed, queried, or trained on. Encryption keys are generated in hardware, per VM, and not exportable.

Enhanced Innovation

Confidential Computing can unlock computing scenarios that have previously not been possible. Organizations will now be able to share confidential data sets and collaborate on research in the cloud, all while preserving confidentiality.

Lift-and-shift - Simple for everyone

Our goal is to make Confidential Computing easy. The transition to Confidential VMs is seamless—all GCP workloads you run in VMs today, can run as a Confidential VM. One checkbox—it's that simple.

Protection against advanced threats

Confidential Computing builds on the protections Shielded VMs offer against rootkit and bootkits, helping to ensure the integrity of the operating system you choose to run in your Confidential VM.

High performance

Built on Google's resilient, scalable global infrastructure and powered by 2nd Gen AMD EPYC™ processors, Confidential VMs offer similar levels of high performance for various workloads, as the standard N2D VMs running on the same infrastructure in the Google Cloud. While encrypting data-in-use and providing added virtualization security, the Confidential instances showed high workload performance running enterprise applications with databases (e.g. PostgreSQL, MySQL, etc.) with only a slight performance delta of about 2-5% in comparison to the equivalent N2D VMs.

Optimize your deployment

Comprehensive management tools to streamline rollout and troubleshoot issues within the console. Pricing for Confidential VMs is based on usage of the machine types, persistent disks, and other resources that you select for your virtual machines. View pricing details.

Google Cloud

For more information visit cloud.google.com/confidential-computing