Confidential Computing

Encrypt data in-use with Confidential VMs and Confidential GKE Nodes

- Breakthrough technology that allows you to encrypt data in use—while it’s being processed
- Simple, easy-to-use deployment that doesn't compromise on performance
- Collaborate with anyone, all while preserving the confidentiality of your data

BENEFITS

Breakthrough in confidentiality

Confidential VMs are a breakthrough technology that allow customers to encrypt their most sensitive data in the cloud while it’s being processed.

Simple for everyone

Google Cloud’s approach allows customers to encrypt data in use without making any code changes to their applications or having to compromise on performance.

Enabling new possibilities

Confidential Computing can unlock scenarios which previously have not been possible. Organizations will be able to collaborate, all while preserving the confidentiality of their data.

Key features

Real-time encryption in use

Google Cloud customers can encrypt data in use, taking advantage of security technology offered by modern CPUs (e.g., Secure Encrypted Virtualization extension supported by 2nd Gen AMD EPYC™ CPUs) together with confidential computing cloud services. Customers can be confident that their data will stay private and encrypted even while being processed.

Lift and shift confidentiality

Our goal is to make Confidential Computing easy. The transition to Confidential VMs is seamless—all workloads you run today, new and existing, can run as a Confidential VM. You do not need to make any code changes to your applications to use Confidential VMs. One checkbox—it’s that simple.

Enhanced innovation

Confidential Computing can unlock computing scenarios that have previously not been possible. Organizations will now be able collaborate on research in the cloud across geographies, across competitors, all while preserving confidentiality.

All features

Real-time encryption in use	Google Cloud customers can encrypt data in use, taking advantage of security technology offered by modern CPUs (e.g., secure encrypted virtualization supported by 2nd Gen AMD EPYC™ CPUs) together with confidential computing cloud services. Customers can be confident that their data will stay private and encrypted even while being processed.
Lift and shift confidentiality	Our goal is to make Confidential Computing easy. The transition to Confidential VMs is seamless—all workloads you run today, new and existing, can run as a Confidential VM. You do not need to make any code changes to your applications to use Confidential VMs. One checkbox—it's that simple.
Detection of advanced persistent attacks	Confidential Computing builds on the protections Shielded VMs offer against rootkit and bootkits. This helps ensure the integrity of the operating system you choose to run in your Confidential VM.
Enable innovation	Confidential Computing can unlock computing scenarios that have previously not been possible. Organizations will now be able collaborate on research in the cloud, all while preserving confidentiality.

High performance	Confidential VMs offer similar performance to standard N2D VMs. Explore tech docs and whitepapers.

Encrypt workload data in-use with Confidential Google Kubernetes Engine Nodes

Overview

Confidential GKE Nodes is built on top of Compute Engine Confidential VM, which encrypts the memory contents of VMs in-use. Encryption-in-use is one of the three states of end-to-end encryption.

When you enable Confidential GKE Nodes on a cluster or on a node pool, data in workloads running on the confidential nodes is encrypted-in-use. For visibility over your control plane, use Access Transparency.

You can enable Confidential GKE Nodes when doing one of the following:

- Create a new cluster
- Create a new node pool
- Update an existing node pool

You cannot update an existing cluster to change the cluster-level Confidential GKE Nodes setting.

The following table shows you the GKE behavior that applies when you enable Confidential GKE Nodes at the cluster level or at the node pool level:

Confidential GKE Nodes setting	**How to configure**	**Behavior**
Cluster-level	Create a new cluster	All nodes in the cluster in any node pool use Confidential GKE Nodes. You cannot do the following: • Disable Confidential GKE Nodes for a new or existing node pool in the cluster • Disable Confidential GKE Nodes on the cluster

		• Enable Confidential GKE Nodes on existing clusters
Node pool level	• Create a new node pool • Update an existing node pool	You can only configure Confidential GKE Nodes for node pools when this feature disabled at the cluster-level.