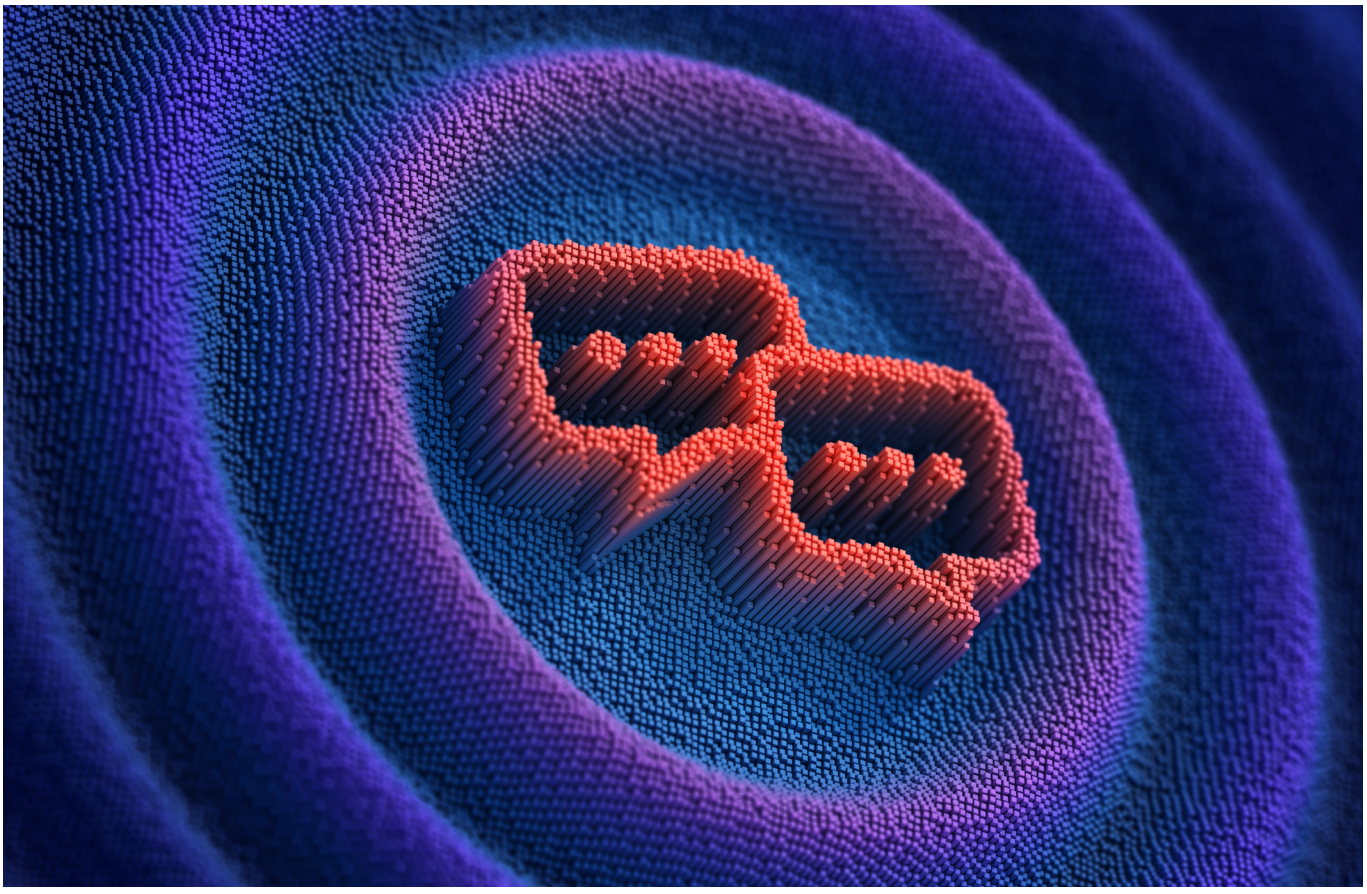
Google Cloud | SYMPHONY

Symphony: Elevating financial communication with Google Cloud's Confidential Computing

October 2025



SYMPHONY

Symphony uses Google Cloud's foundational built-in security controls, specifically Google Cloud Confidential Space and FIPS 140-2 Level 3 compliant Cloud Hardware Security Modules (HSM), to meet and even exceed on-premise security for financial communication. This allows Symphony to offer a fully-managed SaaS platform with features like confidential compute and zero-access operations, giving customers ultimate control over their data while reducing operational burden and enabling secure innovations like AI.

Symphony is a pioneer in secure communication and collaboration, serving as the central hub for information exchange among financial institutions worldwide.

Millions of messages traverse Symphony's Messaging platform daily, playing a mission-critical role in facilitating seamless communication and collaboration across financial institutions. Symphony achieves this while also maintaining high performance, essential for keeping markets moving. The resilience, scalability, and security of the platform are paramount to ensuring financial institutions can rely on Symphony as the trusted foundation for their secure communication needs.

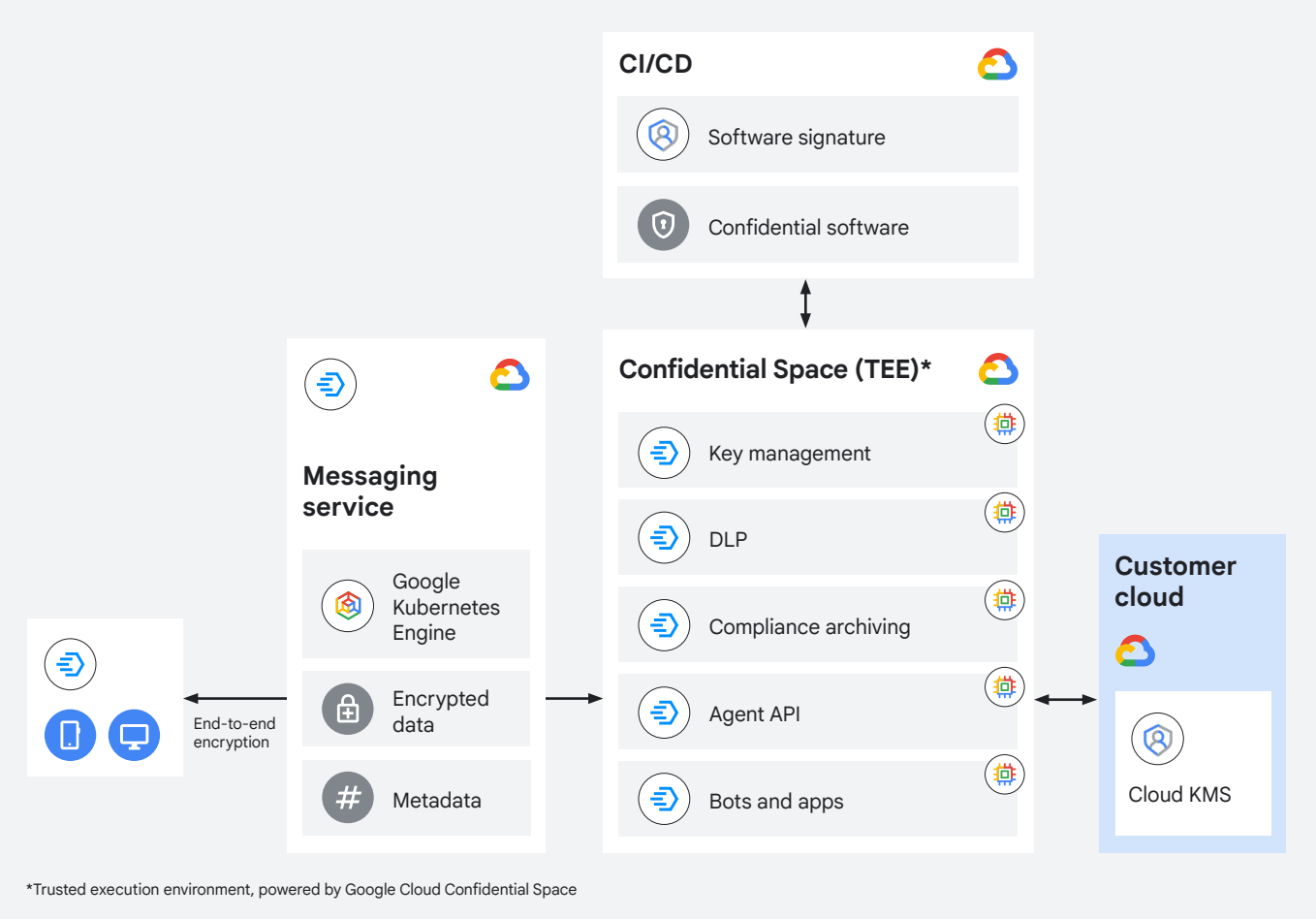
Security evolutions: Paving the way for confidentiality

In the face of evolving security landscape and the increasing demand for cloud-native agility, Symphony has undertaken a significant evolution in its security posture. This strategic transition to a fully managed software-as-a-service (SaaS) model addresses the inherent challenges of managing on-premise infrastructure for sensitive messaging services. This shift brings numerous benefits, including automated upgrades and patching, rapid integration, and streamlined configuration of new services. Furthermore, Symphony Messaging offers integrations with cloud-native services such as identity providers (IdP), HSMs, and Data Loss Prevention (DLP), providing a comprehensive cloud security ecosystem.

The critical first step: Secure key management in the cloud

The initial phase of this undertaking focused on building a secure cloud infrastructure for managing sensitive data. This critical first step was the implementation of a new key manager operating model that allowed for seamless integration with cloud-based HSMs.

This advancement allowed Symphony to move workloads, such as cryptographic operations, to the cloud. By securely managing encryption keys in cloud HSMs, Symphony laid the groundwork for future cloud migrations. This initial success **paved the way for the capability to move other sensitive workloads to the cloud, including advanced functions powered by Symphony workflow automation** (known as Symphony bots), **AI agents, and crucial processes like content export,** ensuring that even as components moved to the cloud, the highest level of data protection was maintained from the Symphony Confidential Cloud.



Confidential Cloud infrastructure

Symphony's Confidential Cloud infrastructure provides security and confidentiality levels that are equivalent to, or even exceed, those of an on-premise deployment. This is achieved through the utilization of the latest cutting-edge security and privacy technologies, specifically Google Cloud Confidential Space, and by maintaining a clear **separation of duties** across the platform's operation.

Key aspects of Symphony's Confidential Cloud include:

Secure enclaves and TEE:
The platform achieves security equivalent to on-premise deployments by operating sensitive workloads within secure enclaves based on **Google Cloud Confidential Space**. This TEE ensures a highly protected execution environment where the integrity and confidentiality of the code and data are protected and isolated from the underlying operating system and hypervisor. This means data remains encrypted even while being processed in memory, rendering it impossible for anyone, including the cloud provider, to access in-memory data in plain text.

Zero-access operations:
Symphony operates sensitive workloads on behalf of the customer with **no direct access to confidential data.** Remote access to the workload, even by Symphony personnel, cloud administrators, SREs, or Google Cloud staff, is blocked – reinforcing true data isolation and significantly reducing the risk of insider threats.

Customer data control and key management:
Customers retain full and continuous control over their confidential data. This is reinforced by **customer control of cryptographic keys, secured using Google Cloud HSM, which is FIPS 140-2 Level 3 compliant**. Without access to these customer-managed HSM keys, data cannot be decrypted, aligning with stringent data regulation requirements. Furthermore, customers can disable data access at any point.

Secured and signed software:
Symphony delivers signed immutable images for all workloads. These images are rigorously scanned, hardened, and then executed on the secure compute cluster. This process prevents unauthorized tampering or access by operators and ensures that all software running in the Symphony Confidential Cloud is certified. This allows customers to verify the software's origin and audit it in Symphony's secured registry.

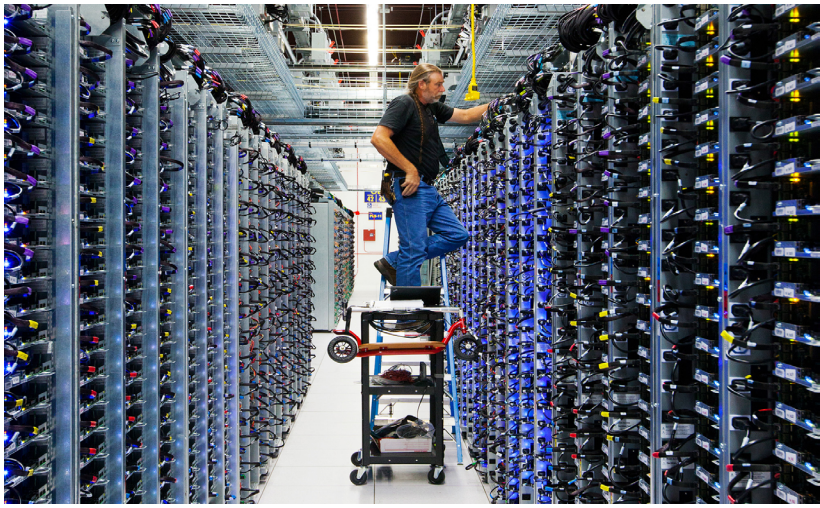
Verifiable attestation:
This process ensures the integrity of the execution environment. Workloads obtain a cryptographically signed attestation token from Google's service. This token provides verifiable proof that the workload is running on confidential infrastructure and has not been compromised, allowing customers to confirm its authenticity at any time.

Customer-defined access control:
This feature enables granular control over data access. Customers use the Symphony Admin Console to configure confidential workloads to impersonate a user identity. Access is granted only after verifying the attributes contained within the attestation token. This mechanism allows customers to precisely define permissions, revoke access rights as needed, and ensure sensitive data is exclusively delivered to trusted confidential workloads.

Secure connectivity:
I/O connectivity is explicitly granted, and all connections within the Symphony Confidential Cloud, as well as with customer cloud/on-premise environments, remain private, minimizing potential attack surfaces.

Powered by Google Cloud Confidential Space

Symphony Confidential Cloud is powered by Google Cloud Confidential Space. Google's underlying architecture has been independently reviewed and validated as a secure platform by NCC Group. Symphony operates the Confidential Cloud platform, diligently maintaining the secure environment and delivering these advanced capabilities to its financial institution clients.



Benefits

This advanced security posture positions Symphony as a **leader in secure financial communication**, offering a highly compelling value proposition to its customers.

Trust and compliance:
By achieving or exceeding on-premise security and confidentiality levels, Symphony instills deep trust in its financial institution clients. This is crucial for an industry with stringent regulatory requirements and high-stakes data. The emphasis on customer control over data and verifiable attestation further reinforces this.

Reduced operational burden and total cost of ownership (TCO) for customers:
The transition to a fully-managed SaaS model, combined with the robust security provided by Google Cloud Confidential Space, significantly reduces the operational burden and TCO for customers. They no longer need to manage complex, expensive on-premise security infrastructure for their communication needs.

Agility and innovation:
By offloading infrastructure management and leveraging the cloud's inherent scalability and flexibility, Symphony can accelerate its own innovation and integration of new services, offering a more agile and responsive platform to its customers.

Future-proofing for AI and Symphony's agentic framework:
The capability to securely move sensitive workloads, including AI-powered agents, to the cloud, opens up new possibilities for financial services, enabling confidential AI-driven insights and automated compliance checks. By leveraging its Confidential Cloud, Symphony ensures that AI models are **not trained on customer data**, and more importantly, that this data is **never exposed to the provider**.

Cloud security:
The unique Confidential Cloud infrastructure, powered by Google Cloud Confidential Space, combined with Symphony's encryption model provides Symphony with a strong competitive differentiator in the market. It allows Symphony to offer a level of data protection that few, if any, competitors can match in a public cloud environment, setting a new standard for cloud security in financial services.

Network of confidential AI agents:
By combining Symphony's agents and directory services with its Confidential Cloud and emerging standards like the agent-to-agent protocol, the platform is uniquely positioned to provide a confidential network of AI agents. This allows agents from different firms to securely discover and communicate with each other through a private channel.

In essence, Symphony benefits from a **highly secure, compliant, efficient, and forward-thinking Google Cloud platform** for financial communication, enabling institutions to leverage the benefits of cloud-based services without compromising on their critical security and privacy requirements.

Google Cloud

Learn more at symphony.com