CallCenter STUDIO

Google Cloud Secures Your Data

Secure your data by using the most trusted cloud infrastructure.

Contact us

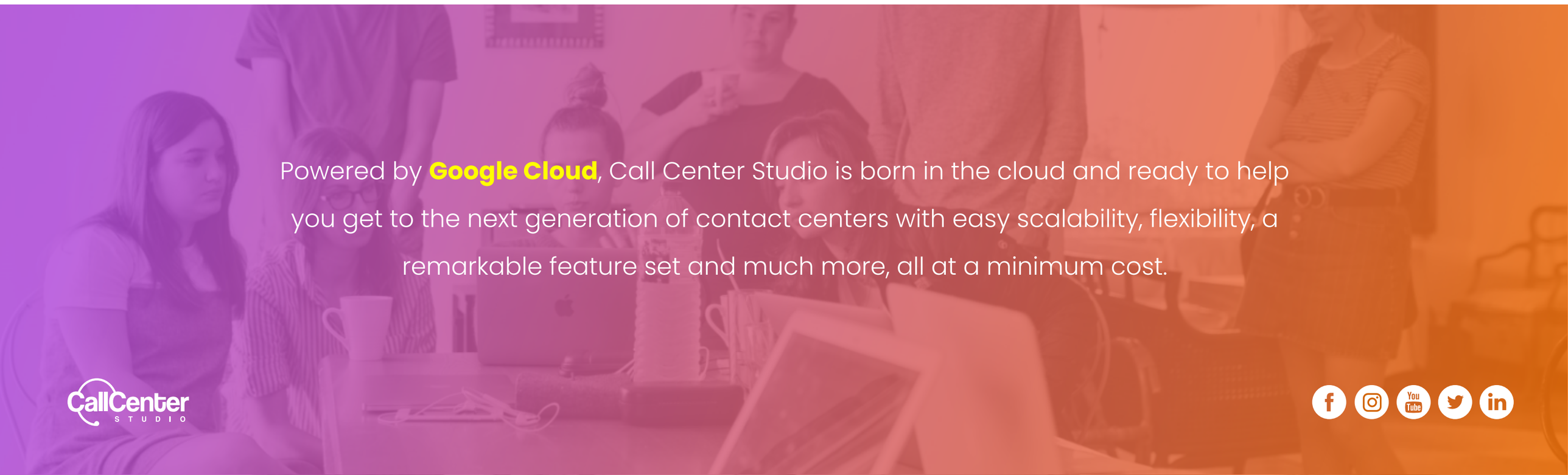
Visit our website for more

Overview

Google Cloud aims to be the most trusted cloud system in the world. To achieve this mission, Google Cloud:

1. Establishes a verifiable secure foundation
2. Delivers visibility and transparency in operations
3. Verifies trusted third-parties
4. Simplifies controls
5. Re-invests in its technology

Happy customers



Powered by **Google Cloud**, Call Center Studio is born in the cloud and ready to help you get to the next generation of contact centers with easy scalability, flexibility, a remarkable feature set and much more, all at a minimum cost.

CallCenter STUDIO

Shield Your Data with Google Cloud

An attacker tries to get your data, take over your resources and get your credentials. To help keep your data safe, Google Cloud provides shielded virtual machines to give you insurance of your data's safety. So, how does this process work?

Shielded VM extends the defense-in-depth model starting from the very lowest level. Because if you can not trust your operating system you can not trust things running on top of it as well.

Starting from the infrastructure of your system, Google Cloud then applies verifiable security to each layer of the operation. This way, you can rest assured that your data storage system is protected at every single layer from attackers.

Google Cloud's Visibility and Transparency Policies

Google Cloud does not only secure your operations and data but also allows you to request reports on the security of your data. This way, you can trust the safety of your data by knowing the details of the security operations. Google cloud's contractual commitments eliminate the risk of malicious activities by allowing you finger-tip access to all your data.

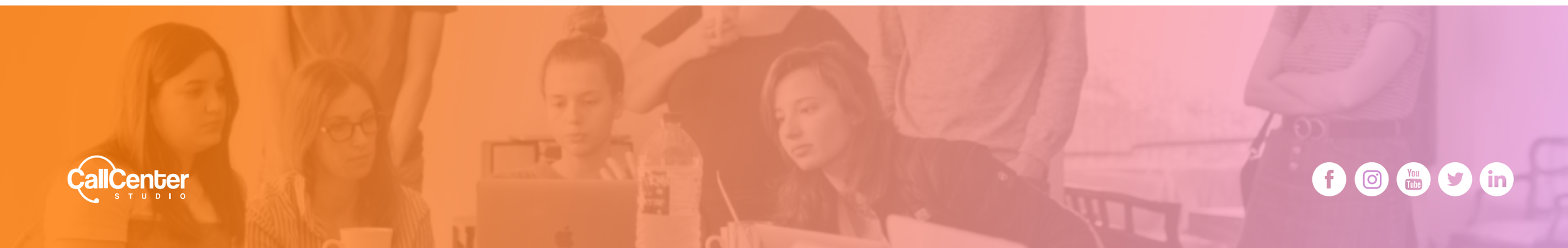
The level of security is fully under your control, and it can be increased at anytime by giving Google permission to track and report who accessed the data, when and where it was accessed, and what was accessed. Access transparency makes Google Cloud's security unique because you can expand your visibility and control using your cloud provider.

Cloud Security Command Center

Meet your security needs with a flexible platform to detect and respond to any threat targeting your cloud resources. Reducing risk by better understanding and managing policies is so easy with Google Cloud platform. Google Cloud automatically scans your GCP infrastructure to bring configuration issues to the surface

Context-Aware Access

Google Cloud unifies access management for apps and infrastructure. This way you are enabled to access your system from any device and high-level security will be activated for all of them. Conveniently, you can use your phone as a security key enhancing your account protection.



Security in the Cloud & Security Services

Google Cloud's security system is highly proactive with advanced phishing, malware protection, and a security sandbox. If there is a chance of any threat, you will be able to place your data into quarantine and take necessary actions to preserve the security of your operations.

Along with its proactivity, Google Cloud is highly intelligent and enables collaborations without security concerns. You can easily save and share investigations in the security center investigation tool, take ownership of alerts in the alert center, and create rules to automate actions in the security center investigation tool.

The simple interface of the product allows you to take security actions quickly. With just a few clicks you can run Data Loss Prevention, gain insights into the security status of your APIs, monitor Event Threat Detection, and manage with Security Health Analytics.

Google Cloud's Security Reports and Certificates

Forrester Research names Google Cloud a Leader in The Forrester Wave™ : Data Security Portfolio Vendors, Q2 2019 report.

Google Cloud regularly undergoes independent verification of security, privacy, and compliance controls, so that it can help you meet your regulatory and policy objectives.

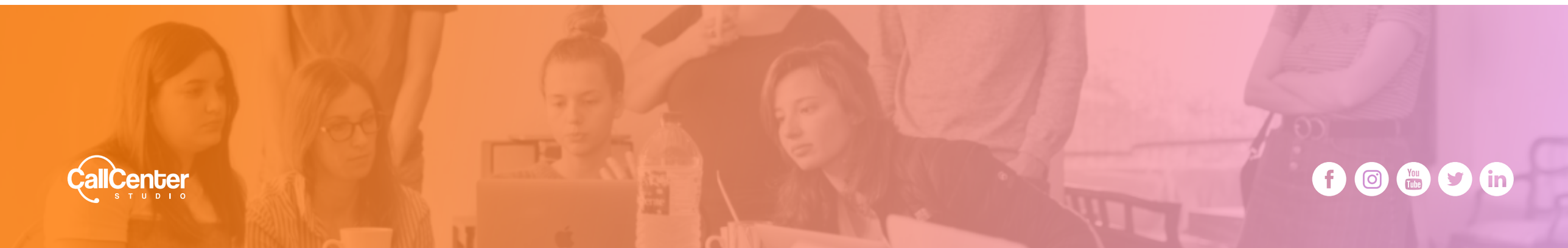
ISO/IEC 27001 outlines and provides the requirements for an information security management system (ISMS), specifies a set of best practices, and details the security controls that can help manage information risks.

The ISO/IEC 27017 gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

- Additional implementation guidance for relevant controls specified in ISO/IEC 27002
- Additional controls with implementation guidance that specifically relate to cloud services.

ISO/IEC 27018 relates to one of the most critical components of cloud privacy: the protection of personally identifiable information (PII). This standard focuses on ways on security controls for public-cloud service providers that process PII:

- Builds upon existing ISO/IEC 27002 controls by adding specific items for cloud privacy
- Provides entirely new security controls for personal data



The PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection. The Standards Council was established by the major credit card associations (Visa, MasterCard, American Express, Discover, JCB) as a separate organization to define appropriate practices that merchants and service providers should follow to protect cardholder data. It is this council of companies that created the Payment Card Industry (PCI) Data Security Standards (DSS).

Google Cloud undergoes an annual third-party audit to certify individual products against the PCI DSS. This means that these services provide an infrastructure upon which customers may build their own services or applications which store, process, or transmit cardholder data.

The Cloud Security Alliance is a non-profit organization whose mission is to “promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”
The CSA’s Security, Trust & Assurance Registry Program (CSA STAR) is designed to help customers assess and select a Cloud Service Provider through a three-step program of self-assessment, third-party audit, and continuous monitoring.

Google Cloud has achieved the third-party assessment-based certification (CSA STAR Level 2: Attestation) for Google Cloud Platform (GCP) and G Suite, resulting in a CSA Star SOC2+ report.

The SOC 2 is a report based on the Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) existing Trust Services Criteria (TSC). The purpose of this report is to evaluate an organization’s information systems relevant to security, availability, processing integrity, confidentiality, and privacy.

Contact

T +1 512 309 5001 | +44 20 8144 4804

M info@callcenterstudio.com

Follow us on social media!