Information Security @ CANdata

Service Providers, Security Features and Responsibilities

CANdata provides applications and support for applications that run on third party SAAS cloud hosting services (Google Cloud Services), taking fullest advantage of the latest in cloud storage security and reliability, in a kubernetes “code as infrastructure” platform across Google Cloud services.

CANdata outsources many infosec and infrastructure services to Google Cloud Services as they are a world leader technology provider that is both standards compliant and responsive to industry change.

Structural Ownership

Item	Responsible Player With Notes
Application • code maintenance • customisation • support	**CANdata** and our internal development team CANdata developer and support access to data adheres to Google’s Single Sign On - utilising OAuth2 standard
Cloud hosting / Container Hosting • data storage • physical access security • network access • security intrusion detection • standards compliance • fail-over protection • backup services	Our contracted service provider is **Google Cloud Services**, applications are run from isolated Kubernetes containers within. This is commonly referred to as “code as infrastructure”. Google Cloud Security https://cloud.google.com/security Google Infrastructure Security Design https://cloud.google.com/security/infrastructure/design Google Container Security (Where your applications run) https://cloud.google.com/containers/security CANdata is responsible to ensure that our cloud service providers have met common I.T. standards for cloud service provisions.
Standards Compliance for Data Centres	**Google Cloud Services** is responsible to maintain compliance. **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 **Google Cloud ISO/IEC 27001 - Expires May 2024** https://services.google.com/fh/files/misc/may_2021_gci_iso27001_certificate.pdf Part of the above standard, **ISO/IEC 27017** gives guidelines for information security controls applicable to the provision and use of cloud services, as well as implementation guidance. **Google Cloud ISO/IEC 21017 - Audit Report available on request** Last updated located here: GCP-[FALL-2020] GCP ISO 27017 - Statement of Applicability..pdf **ISO/IEC 27018** relates to one of the most critical components of cloud privacy: the protection of personally identifiable information (PII) **Google Cloud ISO/IEC 27018 Certificate - Expires May 2024**

	GCP-[SPR-2021] GCP ISO 27018..pdf **CSA STAR** - 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. **Google CSA Start Self Assessment** Details and certificate below https://cloud.google.com/security/compliance/csa-star **SOC 1/2/3 Auditing Standards** For those interested SOC standards followed by Google cloud are available but are not a necessary part of CANdata hosting needs. https://cloud.google.com/security/compliance/soc-1 **PCI DSS** For those interested PCI DSS standards followed by Google cloud are available but are not a necessary part of CANdata hosting needs. This PCI Security 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. 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. **Details of this program** - https://cloud.google.com/security/compliance/pci-dss CANdata is responsible for annually reviewing and ensure Google has maintained its compliance levels with appropriate standards. **Google Cloud Services Standards**  https://cloud.google.com/security
Security within the application itself	CANdata customers control access within the application, CANdata can support them with these functions but they are the client responsibility to maintain.
Data Content	Customer data is owned by customer, co-managed by CANdata and customer within CANdata applications.
Usage / Security Control	The customer is responsible for proper use of provided security rights provisioning tools within application, and to keep API and other usernames, passwords, tokens, private. Communications between customer owned systems and CANdata APIs should always be in an encrypted manner when trading or sending data.

Application to Cloud Communications • End to End Encryption	CANdata applications such as Freight Flow and Customs Flow desktop apps use encrypted communications end to end when communicating with SAAS architecture.
Audit Logging	Google Cloud Services is solely responsible for audit logging and maintains a robust infrastructure for this reason. Details found here: https://cloud.google.com/kubernetes-engine/docs/how-to/audit-logging Logging most relevant to applications hosting security found here: https://kubernetes.io/docs/tasks/debug-application-cluster/audit/

Intrusion Detection Technology by Google

Google has sophisticated data processing pipelines which integrate host-based signals on individual devices, network-based signals from various monitoring points in the infrastructure, and signals from infrastructure services. Rules and machine intelligence built on top of these pipelines give operational security engineers warnings of possible incidents. Investigation and incident response teams triage, investigate, and respond to these potential incidents 24 hours a day, 365 days a year.

https://cloud.google.com/security/infrastructure/design#intrusion_detection

Data / Security Breach Handling

In the unlikely event of a cloud data breach, Google Cloud customer support will proactively inform CANdata of said breach while deploying their forensic process.

Google Cloud data breach handling details found here

https://cloud.google.com/security/incident-response

Proactive Communication Policy - CANdata Customers

CANdata will immediately review extent of any data or security breach, determine if any customer owned data is affected, and proactively provide all details to customer as they come available.

CANdata likewise will hold an internal review with meeting minutes kept, after investigation, to determine and implement correct actions.

Minutes will be shared with affected customers.

Minimal Host OS

Google Kubernetes Engine uses as purpose built OS optimised specifically to run containers known as “COS” Container Operating System. COS is maintained by Google in open source libraries.

Keys are encrypted in transit, and on disk., and all data is encrypted both while stored and while in transit.

Physical Storage Access

CANdata does not store any customer owned data on premises, 100% of customer data is stored in Kubernetes containers or Cloud SQL within **Google Cloud Services** - Nobody at CANdata has physical access to the data centres at Google.

CANdata staff work with data in the cloud when doing database management functions, not on their workstations.

Physical access to Google data centre policies are defined here:
https://cloud.google.com/security/infrastructure/design#secure_low_level_infrastructure

Network Access

CANdata customers have network access only through encrypted or secured connection (Such as HTTPS) to API endpoints, that are mapped solely to their own isolated system. CANdata customers do not have direct access to Google Cloud services infrastructure, and code as infrastructure management access is only available to key people within CANdata itself.

This access is backed up by Google intrusion detection and DDOS/DOS prevention technology.

DDOS / DOS Denial of Service Protection

The sheer scale of Google Cloud infrastructure enables Google Cloud to simply absorb many DoS attacks. That said, GCS offers multi-tier, multi-layer DoS protections that further reduce the risk of any DoS impact on a service running behind a GFE (Google Front End).

https://cloud.google.com/security/infrastructure/design#denial_of_service_dos_protection

Storage and Encryption

Data “at rest” is kept encrypted in the Google Cloud infrastructure Secure Data Storage system.

Deletion of data is handled by schedules rather than instant removal allow recovery from unintentional deletions or critical infrastructure code.

https://cloud.google.com/security/infrastructure/design#secure_data_storage

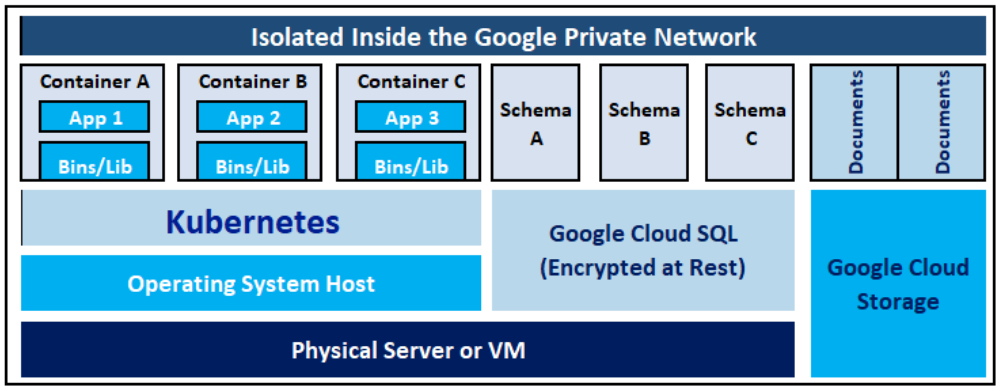
Vulnerability Scanning

Google Container provides CANdata with vulnerability scanning based on the CVE database. https://cve.mitre.org/

https://cloud.google.com/container-registry/docs/vulnerability-scanning

Resource and Workload Isolation

CANdata deploys containers in an isolated infrastructure. Containers are not only isolated from other containers but also isolated from the hardware and the operating system. This structure has significant advantages over previous VMware structures which packaged the OS in the container with the application and data, allowing an intruder to wreak havoc. Now within the container resides only the code for the application. There is nowhere for an intruder to go and nowhere for an intruder to install hidden server processes or malware. Asynchronous communication between the application and database is in a fully encrypted state.



Disaster Recovery / Fail Over

All developers work from a transaction / explicit commit process allowing instant rollback of any changes and which would catch programmer errors. We do not allow developers to directly update databases, the explicit commit process is employed instead.

Google snapshots databases daily for up to 7 days, faster restores.

CANdata has the backup set to backup 100% of the database regardless of age of transactions.

CANdata employs point in time recovery for the period covered between backups during those 7 days.

Redundant drives and data centres are employed by our cloud provider Google.

Google environment failure are Google's disaster recovery teams responsibility, and CANdata will review our environment once Google restores service.

All CANdata server infrastructure is code which is simply redeployed via our standard build routine.