ARCULES

Security by Design in Arcules VSaaS Products

WHITE PAPER

OVERVIEW

Video Surveillance as a service (VSaaS) refers to the leveraging of cloud-native technologies and platform as the foundation ecosystem to provide video surveillance service. Arcules VSaaS product is designed and built from the ground up and deployed as a Software as a Service model using Google Cloud Platform (GCP). Arcules' software components are deployed in the cloud to centrally manage and control all aspects of video recording, streaming, playback and alert for cameras and IoT devices deployed at customer sites.

The overarching basic security objectives that our product strives to achieve include:

Confidentiality

Ensuring that information is only being used or seen by authorized people and processes

Integrity

Ensuring that any changes to the information by an unauthorized user are prevented (or at least detected) and changes by authorized users are tracked and achieved as intended

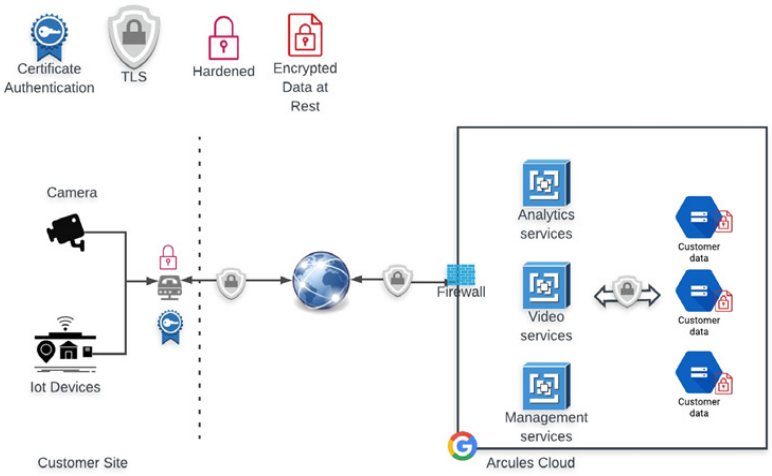
Availability

Ensuring that information and functionality needed is accessible whenever authorized users need them.

These objectives drive a set of best practices in the design and deployment of the product.

This white paper provides an overview of the approach to secure Arcules products.

SECURITY DESIGN PRINCIPLES



As video surveillance functionalities and data are hosted in the public cloud environment, it is imperative to ensure that all aspects of the service delivery and data that the system handled are properly protected end to end. VSaaS products should be designed and built in accordance with the following principles:

Defense in Depth Principle

Security protection is only as strong as the weakest links. To allow for better redundancy, security controls are designed and implemented in each layer of the product system components to:

Data at rest

Leveraging GCP encryption by default for all data at rest, all video and application data are stored encrypted in GCP cloud storage and databases using AES256.

The following reference paper will provide a more in-depth view into GCP encryption by default
https://cloud.google.com/security/encryption-at-rest/default-encryption/

Data in transit

Data communication between devices to and from a customer site to cloud storage and application service-to-service communication are done over Transport Layer Protocol, an end to end encrypted communication protocol designed to prevent eavesdropping, tampering and message forgery with support to mutual authentication between client and server.
https://cloud.google.com/security/encryption-in- transit/#service_integrity_encryption

Network control

Arcules system leverage Google's IP network, a low latency network that is built with highly redundant design. Security services in Arcules environment at the network layer are handled using Google VPC, firewall and DDoS protection, providing for private IP address space and communication over Google private fiber network globally instead of the Internet.

Application identity and access management

Role-based access control is provided within the application for managing access to different functionalities of the application for authorized and authenticated users.

Least Privilege Principle

The least privilege principle is the concept of restricting access rights for users, accounts and computing processes to only those resources absolutely required to perform legitimate activities and operations. Applied to people, this means enforcing the minimal clearance level for the user to perform his/her role. However, least privilege also applies to processes, applications, systems, and devices where each should have only those permissions required to perform an authorized activity.

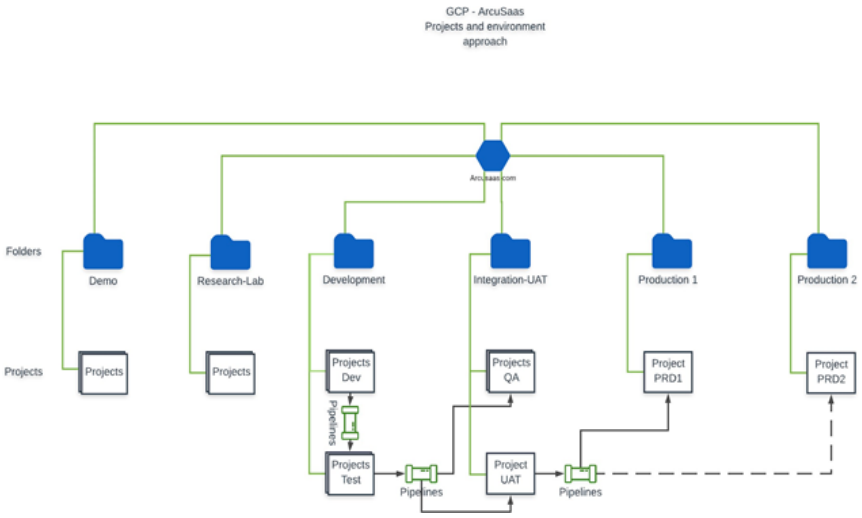
This principle is applied in the design, deployment, and operation of our product in the following areas:

Isolation of customer data

Video data and metadata recorded and stored are logically isolated by customer. This ensures full protection of customer confidentiality and enables regional and international privacy compliance requirements as needed.

Segregation of operating environments

Arcules production environments are segregated from non-production environments. This compartmentalization approach applies best practice for managing access control based on trust level requirements and security profile of the environments. It also allowed for effective fault domain isolation whereby issues in the non-production environment cannot propagate and affect normal production operation



Just-in-time privileges

Service to service communication is authenticated and authorized for specific tasks and activities for the session they are needed, without requiring administrative credentials or exposing the credentials (“privilege bracketing”). The privileges granted are also time-bound and/or bound by the completion of a specific task or process.

Granular traceability

Interactive transactions, service to service communication and transactions are fully logged, encrypted and stored. Security privileges are regularly audited to ensure compliance and risk assurance.

Immutable Infrastructure Principle

Traditionally any security vulnerabilities or incidents issues are dealt with using in place patching of currently deployed code. System mutability prevention and detection are important challenges in security operations as unwanted changes need to be eliminated and the desired state need to be restored quickly. Infrastructure immutability refers to using infrastructure with components that are designed to be destroyed and replaced with new versions whenever a change is necessary.

Arcules product is built with cloud native architecture. It is deployed and managed using Kubernetes, an orchestration and deployment engine for containerized microservices.

Using these technologies allows us to implement immutable infrastructure in the environment: security issues and vulnerabilities can be corrected quickly and simply with automatic deployment of new build and images of a clean next version thereby rendered patching of the environment obsolete.

Applying the immutable paradigm combining with cloud-native technology such as Docker, Kubernetes and modern deployment automation, risk-prone security workflows such as security patching become things of the past. Security vulnerabilities can be mitigated quickly and with minimal disruption services for end-users.

CONCLUSION

Adherence to the above principles are key to the design, build and deployment of VSaaS products to ensure that we can deliver an end to end efficient and secure solution to our customer.

References

GKE Kubernetes security Overview

Google Cloud Platform Security Overview

Encryption at rest in GCP

Encryption in transit in GCP

Application Layer transport security in Google Cloud

ARCULES™

Canon
CANON GROUP

Google Cloud

Arcules
17875 Von Karman Avenue, Suite 450
Irvine, California 92614
info@arcules.com
arcules.com