Using Cloud Security Scanner to Identify App Vulnerabilities

Janani Ravi

CO-FOUNDER, LOONYCORN

www.loonycorn.com

Overview

Cloud Security Scanner to automatically scan apps for common vulnerabilities

Works with App Engine and Compute Engine web applications

XSS, Flash injection, mixed-content, clear-text passwords, use of outdated libraries

Exclude URLs based on patterns

Quick introduction to Forseti Security - open-source security tools for the GCP

Google Cloud Security Scanner

Cloud Security Scanner

Identifies security vulnerabilities in App Engine and Compute Engine web applications

Scanner Vulnerability Classes

- Cross-site scripting
- Flash injection
- Mixed content
- Clear-text password
- Invalid headers
- Outdated libraries

New vulnerability classes constantly being added

Cross-site Scripting (XSS)

Attack where malicious client-side scripts injected into pages

Very common source of vulnerability

Non-persistent (reflected) attacks occur when inputs are not sanitized

Persistent (stored) attacks are able to alter state of the server

Cross-site Scripting (XSS)

Simulates injection attack

Inserts benign text string into user input fields

Then detects if DOM was altered

If yes, vulnerability is flagged

Manual inspection needed to check if vulnerability is exploitable

Flash Injection

Specific type of XSS

Specific to Flash, a proprietary format for multimedia

Injects malicious code into Flash objects

Flash Injection

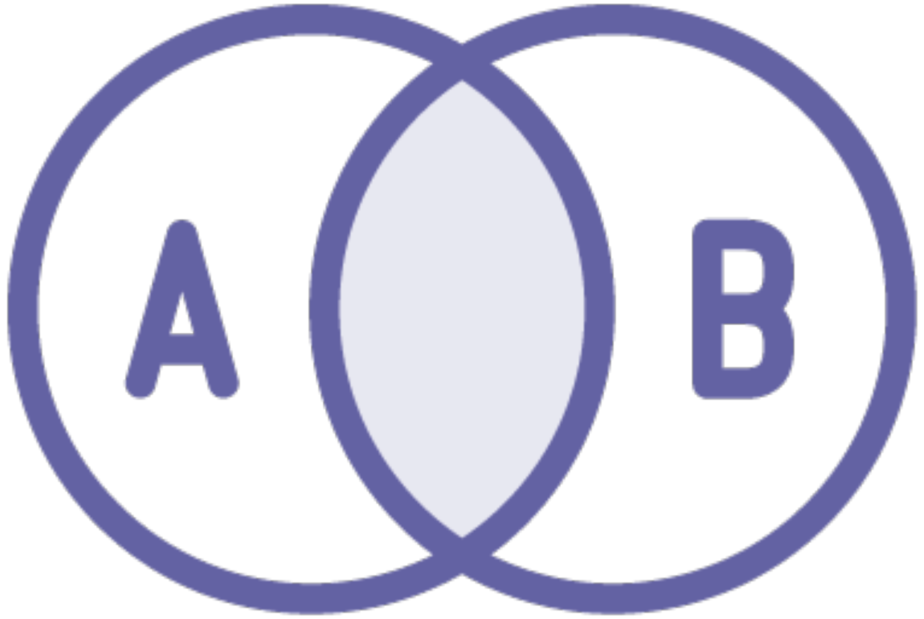
Searches for user-specified parameter reflected back at beginning of response

Known as Rosetta Flash

May be possible for user to trigger execution as though it a legit Flash file provided by the application

App should avoid user controllable data at start of HTTP response

Mixed Content



Occurs when HTML is loaded along with other resources

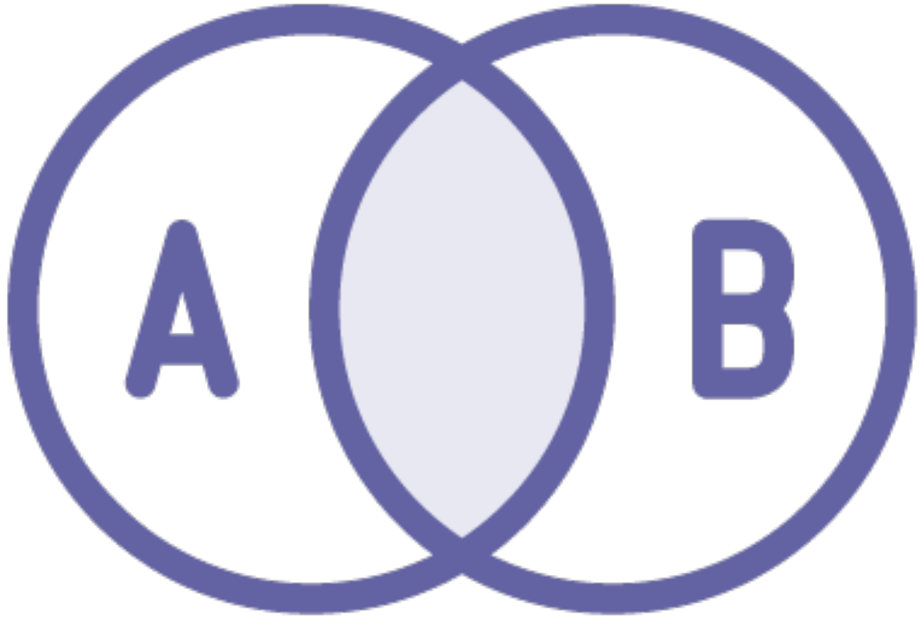
Videos, images, stylesheets, scripts

HTML loaded on secure HTTPS

Other content loaded on insecure HTTP

Browser warning maybe too late

Mixed Content

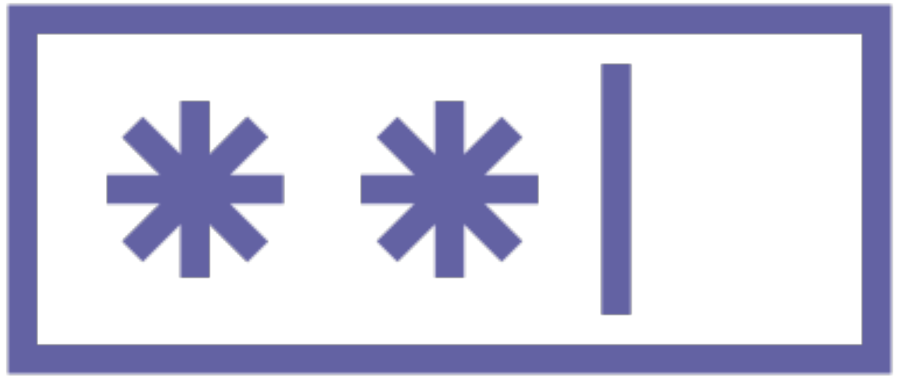


Passively observes HTTP traffic

Detects when HTTP request occurs inside HTTPS page

Should be no `http://` URLs inside `https://` page

Clear-text Password

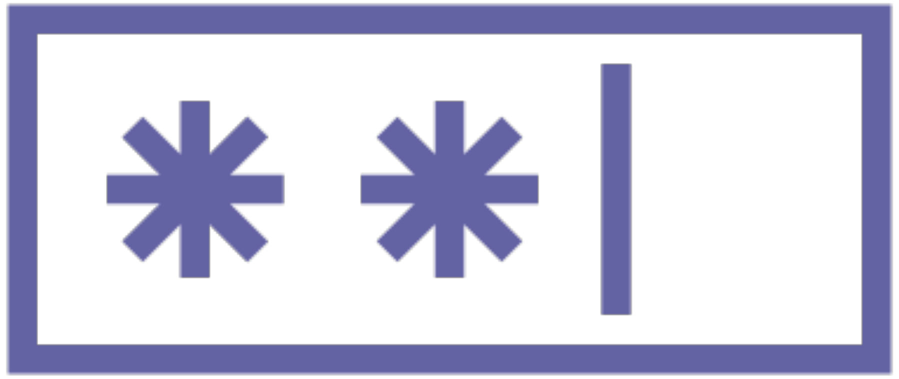


Apps might be transmitting password in clear text

Includes storing password in config file

Also includes encoding e.g. base64

Clear-text Password

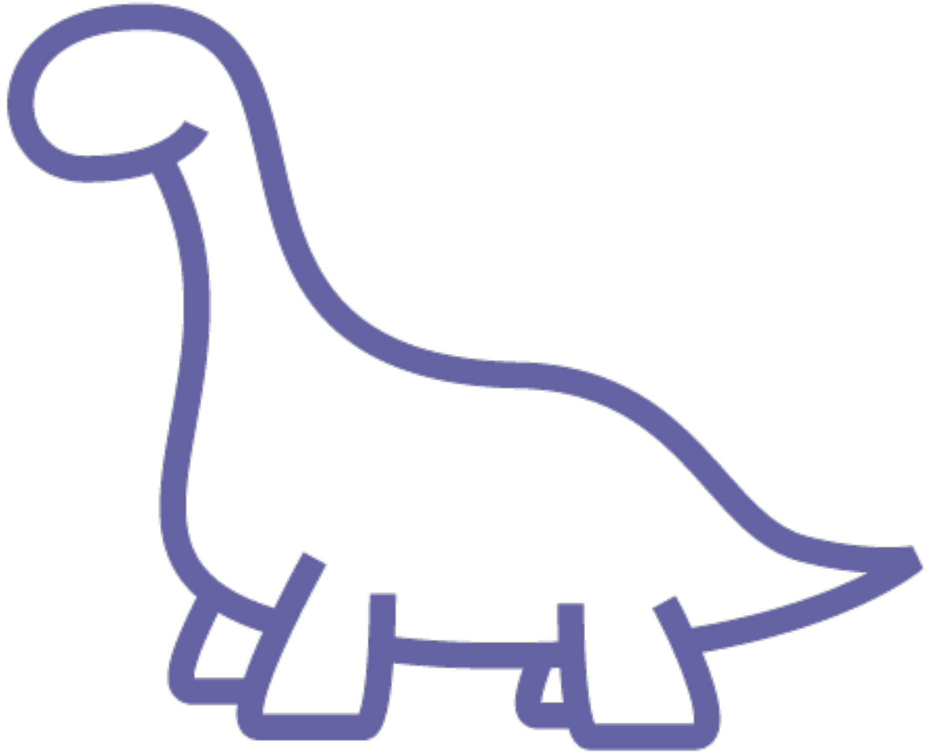


For pages which accept passwords use TLS/SSL certificates

Use HTTPS

Form action should always point to HTTPS URL

Outdated Library Usage



Cloud security scanner maintains list of libraries with known security issues

Signature-based scan attempts to identify version in use

False positives possible

Manually patched libraries will not be detected

Invalid Content-type Header

{JSON}

Browsers deal with files based on their type

Rely on content-type header set by server

Attack could intentionally mis-specify content-type

E.g. upload zip file which is actually HTML with embedded script

Invalid Content-type Header

Compare loaded resource to response header

Content should have the right MIME types specified

JSON responses should have type `application/json`

HTTP header should include `X-Content-Type-Options: nosniff`

Caveats, Restrictions and Pricing

Cloud Security Scanner Usage Caveats

A future scan may report issues that are not reported by the current scan

Some features or sections of your application might not be tested

The Cloud Security Scanner attempts to activate every control and input it finds

May lead to undesirable results

May want to run the scanner in a test environment

Target Restrictions

Filters restrict scan targets to specific App Engine instance

URLs for a different App Engine project or outside domain will result in error

Cloud Security Scanner

Does not execute immediately, may be queued and executed later

Execution time is on the basis of size of your application

Excluding URLs in Scans

The scanner does not request resources that match any of the exclusions

Pattern Matching for Excluded URLs

Based on set of URLs

Parts of Match pattern

- Scheme
- Host
- Path

Cloud Security Scanner Pricing

No additional charges for Scanner

Scanner impacts usage

- Quota limits
- Bandwidth
- API calls to App Engine services

Demo

Using Cloud Security Scanner with App Engine

Demo

Using Cloud Security Scanner with Compute Engine

Forseti Security

Forseti Security

Community-driven, open-source tools that use JSON or YAML rule definition files to audit GCP resources

Features

Track GCP resources using inventory snapshots

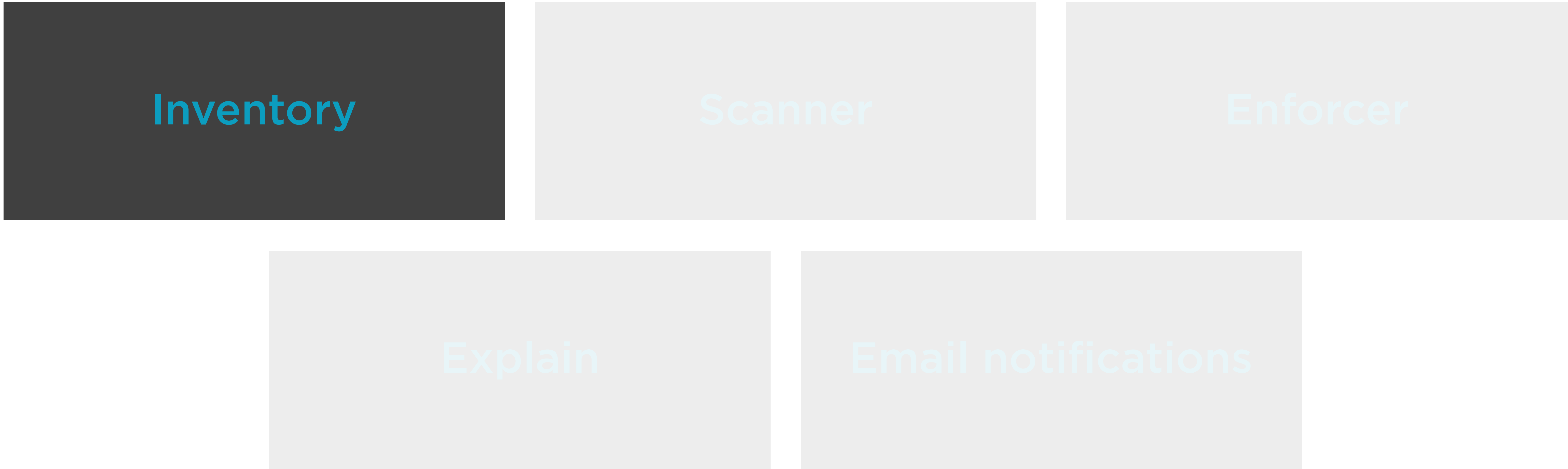
Monitor policies to ensure access controls are set as intended

Enforce rules

Forseti Modules

- Inventory
- Scanner
- Enforcer
- Explain
- Email notifications

Inventory



Takes a snapshot of GCP resources and stores in a Cloud SQL instance

Inventory

Inventory

Scanner

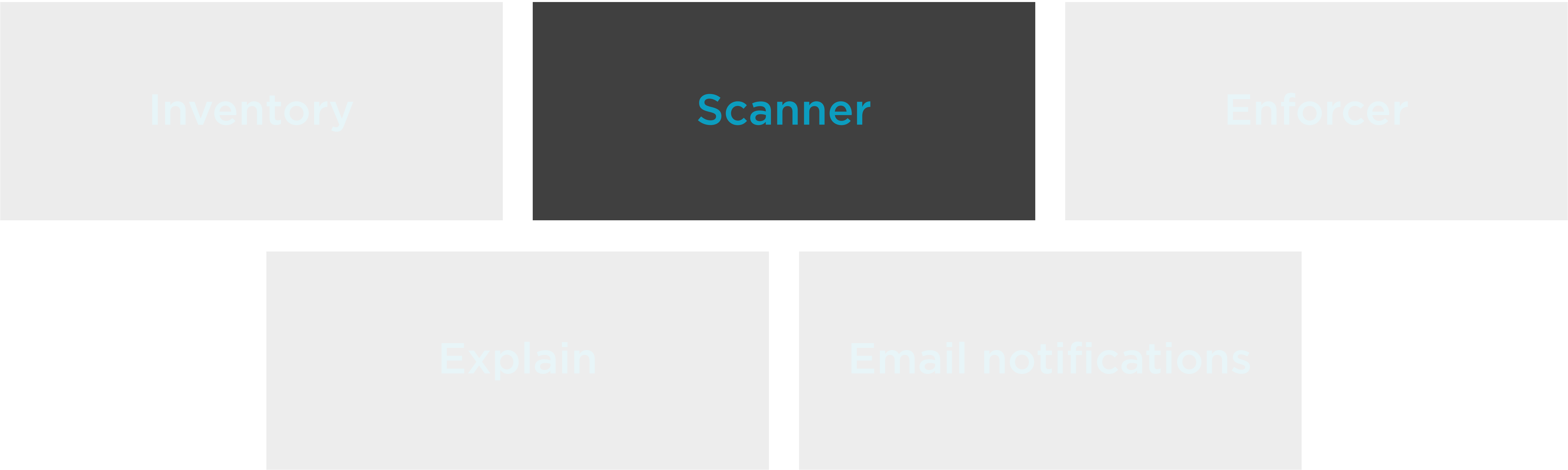
Enforcer

Explain

Email notifications

Used to understand resources used and take actions to conserve resources and minimize security exposure

Scanner



Inventory

Scanner

Enforcer

Explain

Email notifications

Uses inventory data to audit GCP resources like Cloud IAM policies, bucket and BigQuery ACLs

Enforcer

Inventory

Scanner

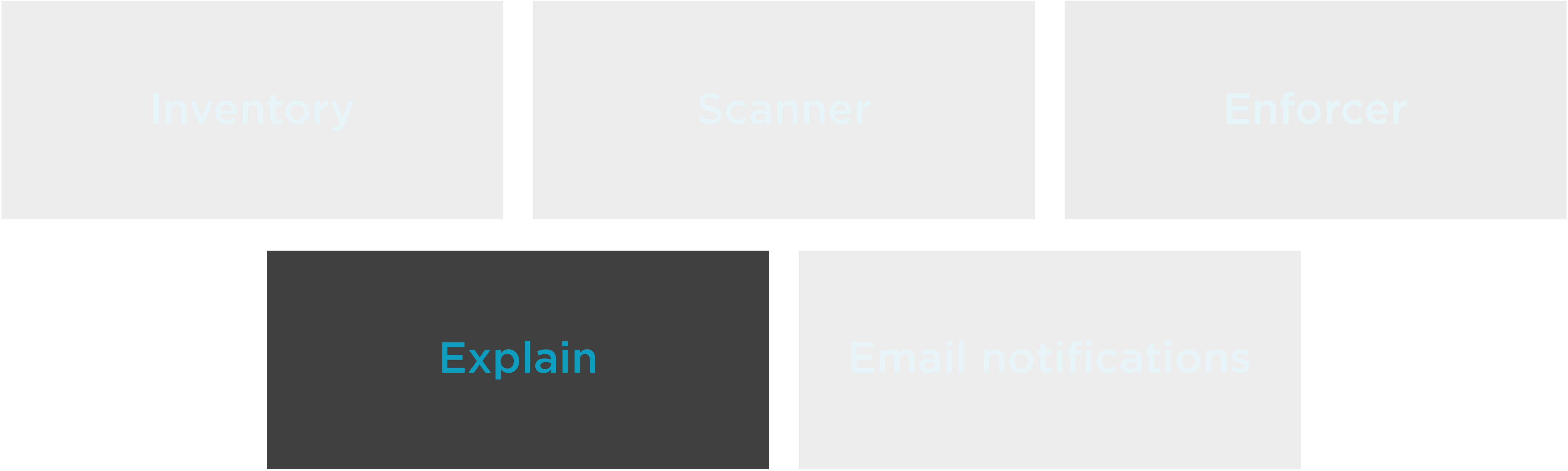
Enforcer

Explain

Email notifications

Enforces firewall policies on a project so it matches the user-defined desired state

Explain



Inventory

Scanner

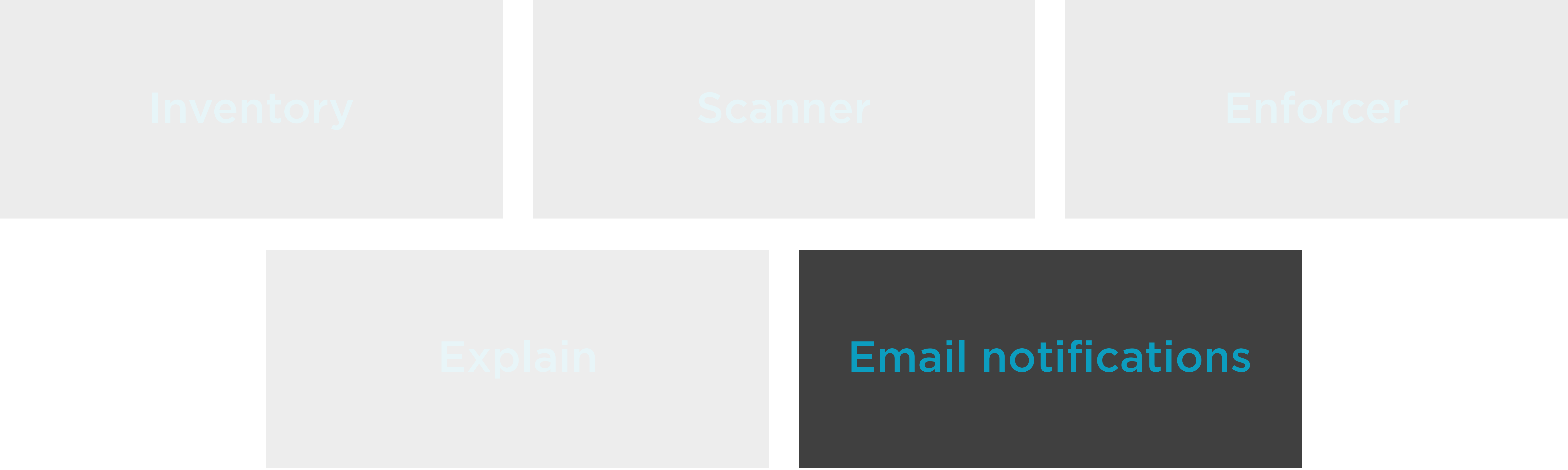
Enforcer

Explain

Email notifications

Provides visibility into who has access to what resources

Email Notifications



Inventory

Scanner

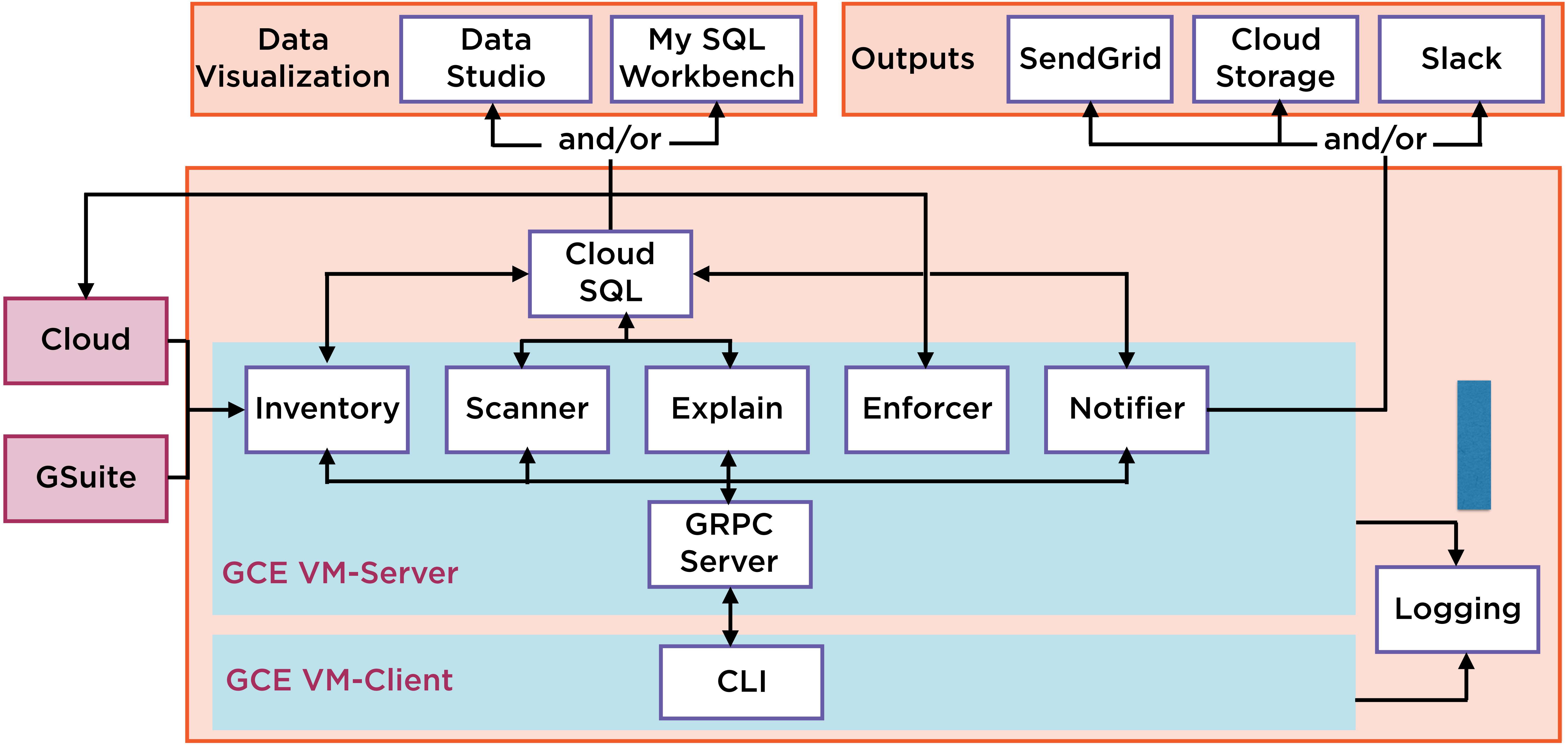
Enforcer

Explain

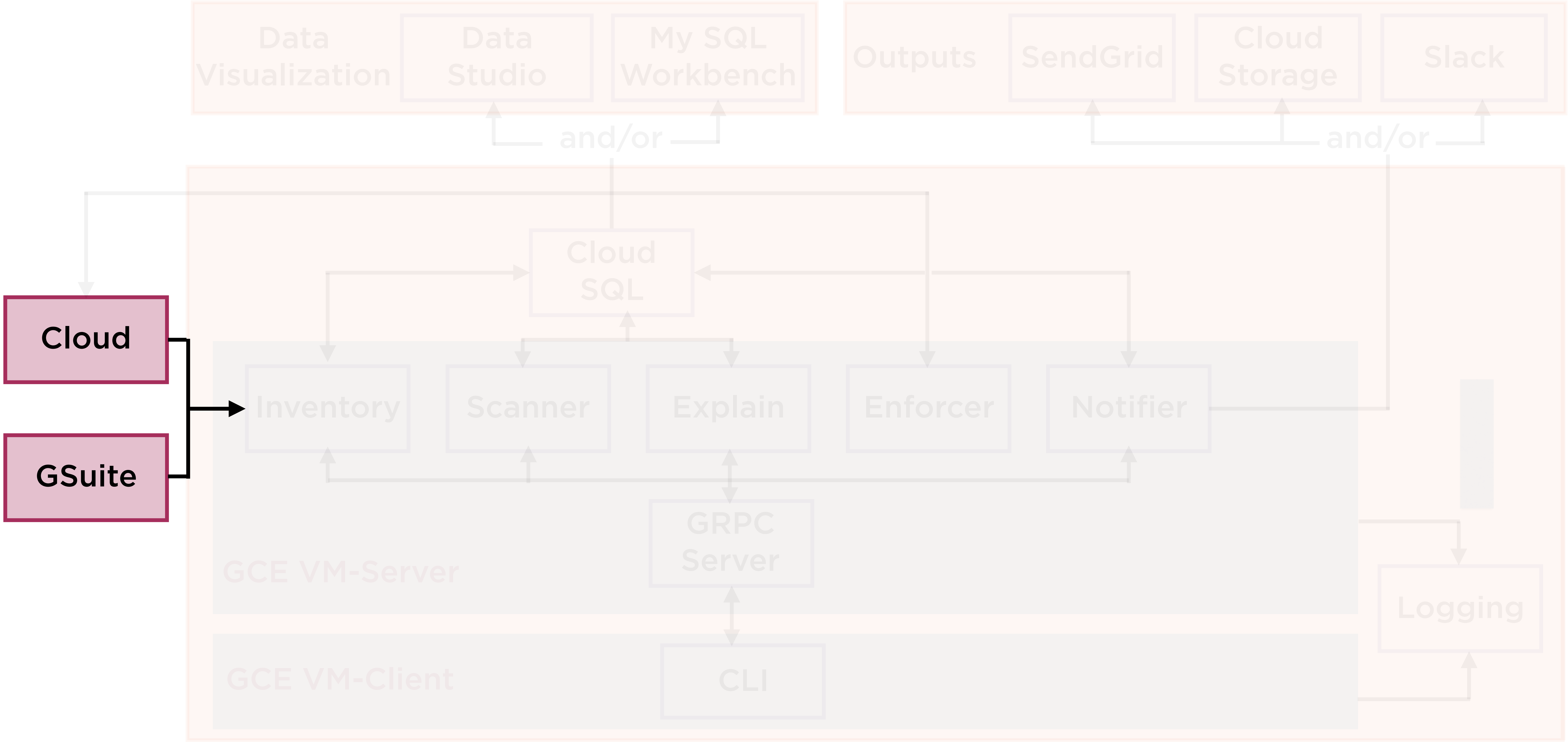
Email notifications

Uses SendGrid to send email notifications for the Inventory and Scanner modules

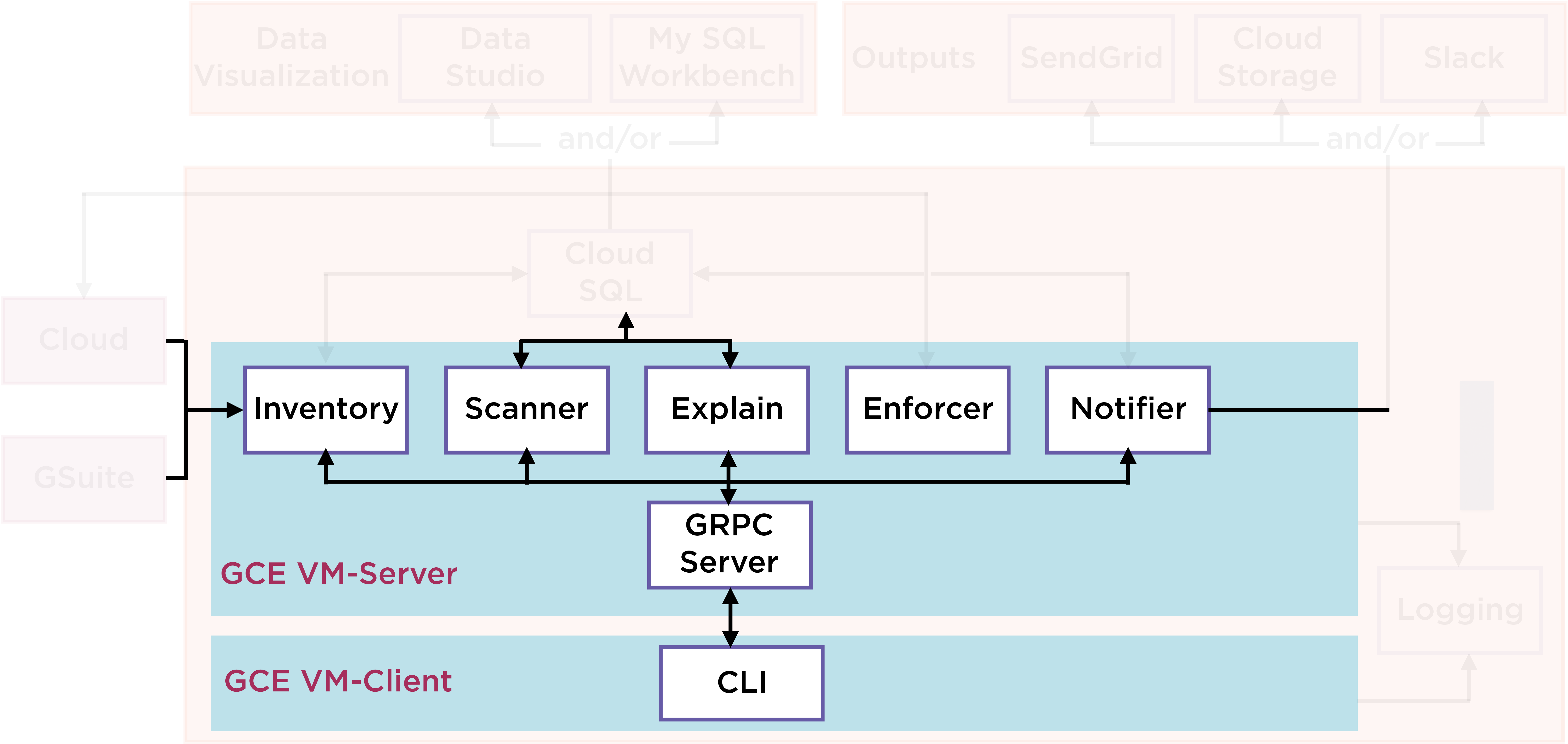
Forseti Architecture



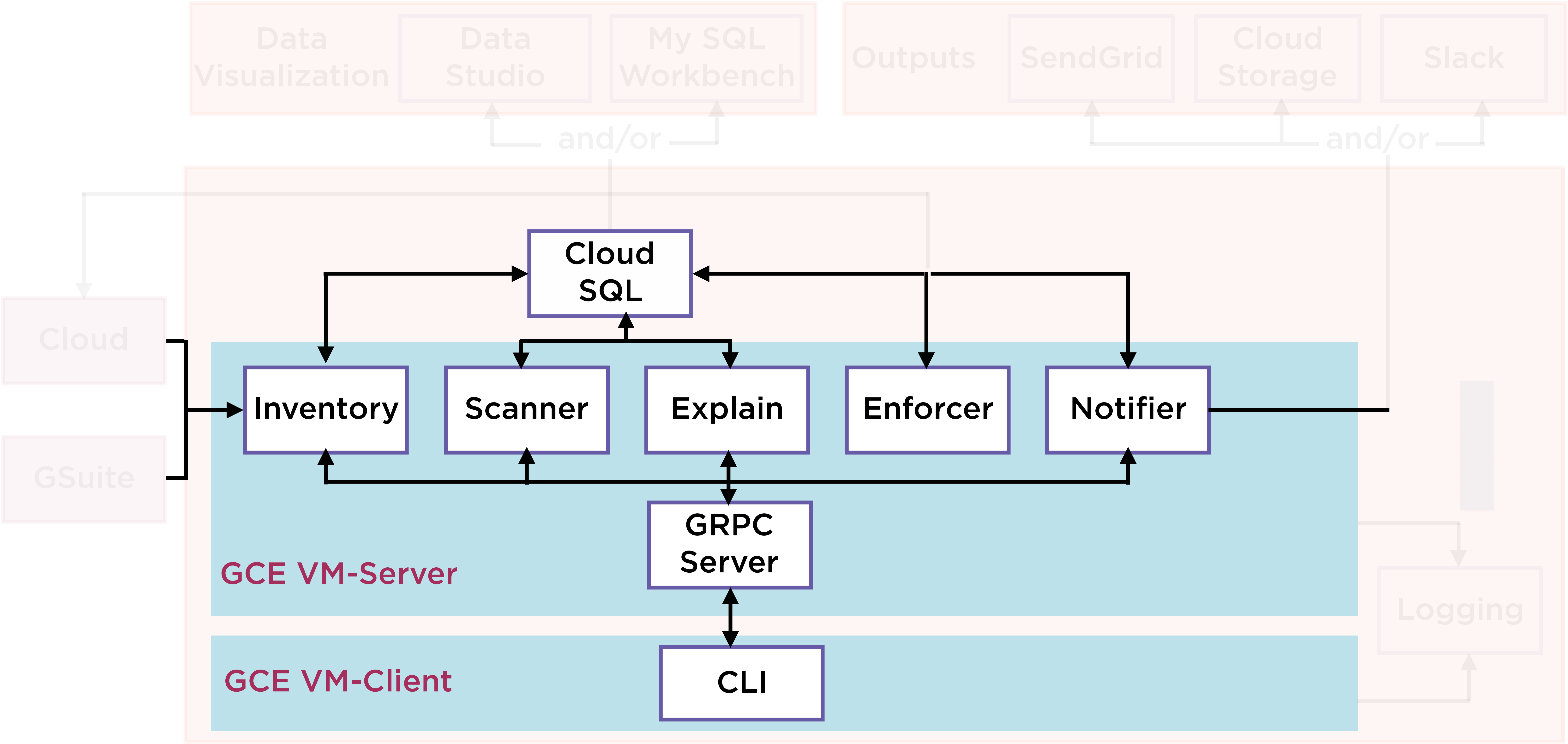
Inputs From the GCP and GSuite



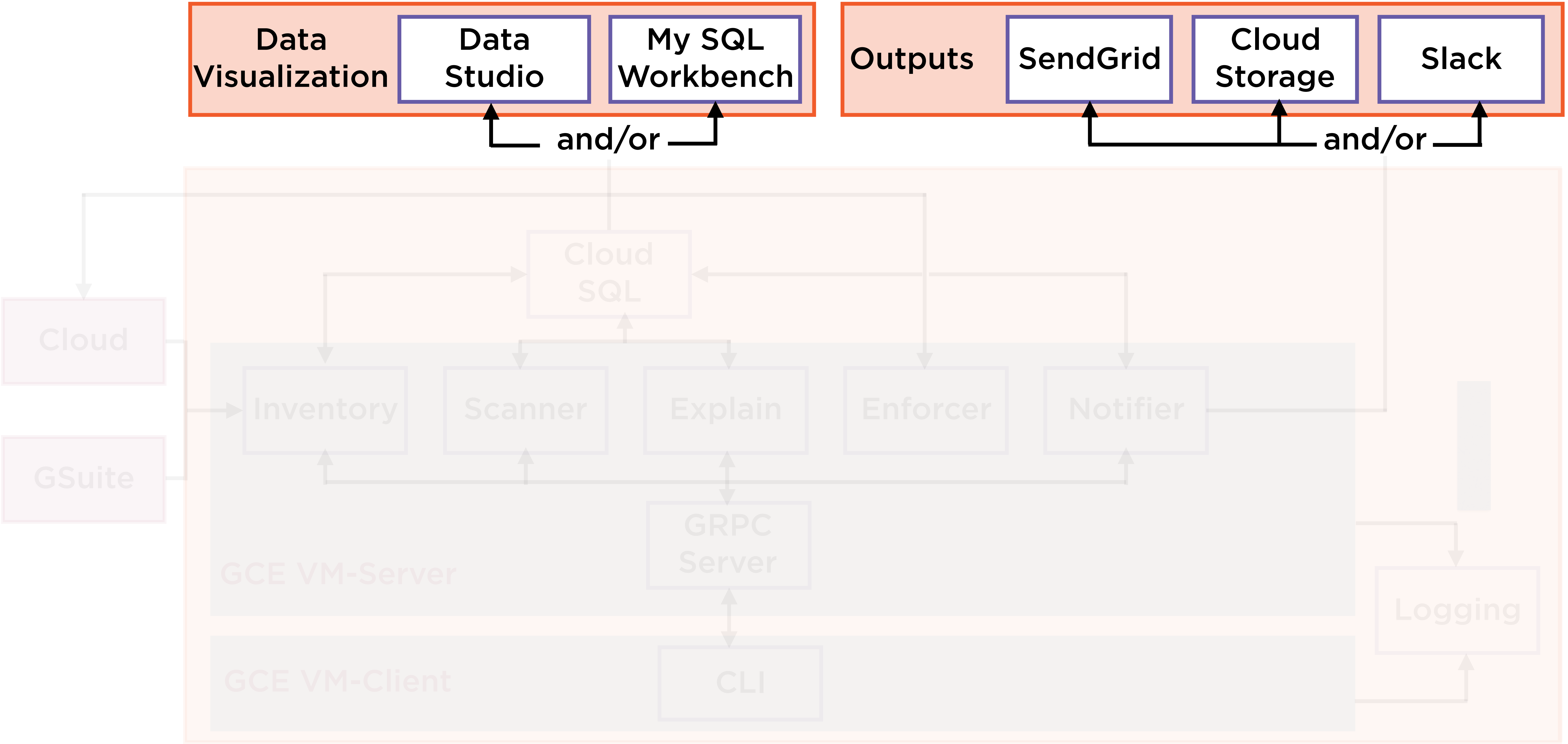
Forseti Modules



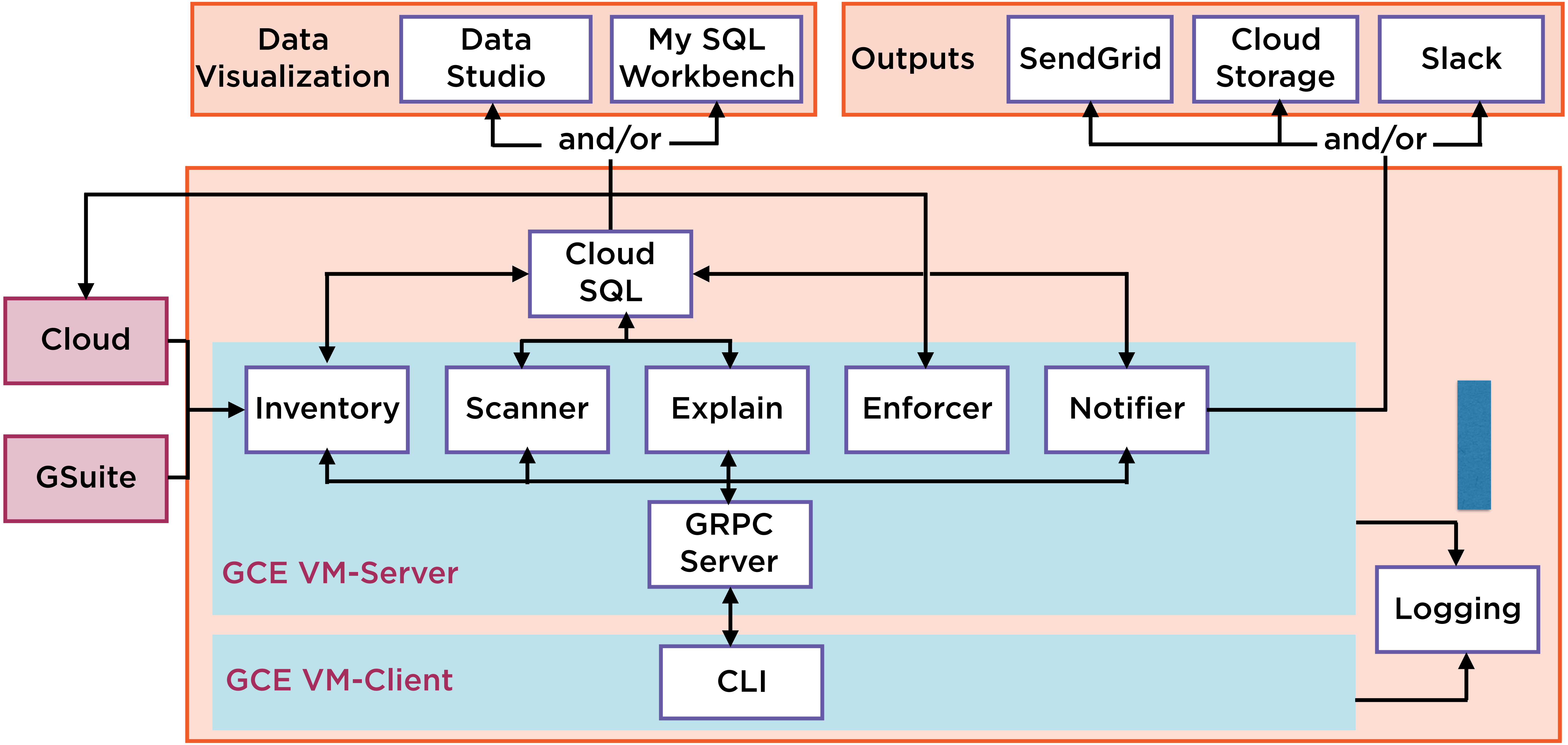
Resource Data Stored in Cloud SQL



Forseti Architecture



Forseti Architecture



Data Model

An additional pool of relational data

Created from the flat JSON data in Inventory

Allow Forseti to more easily understand inheritance between resources

Models allow for easier querying against the entire computed policy

Demo

Installing Forseti security tools

A quick introduction to the Forseti command line interface

Summary

Cloud Security Scanner to automatically scan apps for common vulnerabilities

Works with App Engine and Compute Engine web applications

XSS, Flash injection, mixed-content, clear-text passwords, use of outdated libraries

Exclude URLs based on patterns

Quick introduction to Forseti Security - open-source security tools for the GCP