4.10 Ensure That App Engine Applications Enforce HTTPS Connections

***Sentinel Policy Name:***

* + 4.10 Ensure That App Engine Applications Enforce HTTPS Connections

***Category :***

* + Google Compute Engine/ Google Application Engine

***Description of Policy:***

* + In order to maintain the highest level of security, all connections to an application should be secure by default.
  + Insecure HTTP connections maybe subject to eavesdropping by hackers which can expose sensitive data.
  + When creating an Application using the Google Application Engine, an application version must be selected: Either Standard version or Flexible version. This policy will ensure that security of the Application is strong from a Cyber Security standpoint.

***Sentinel Policy Restriction:***

* + We are checking the ensure that applications created via the Google Application Engine enforce HTTPS connections (as opposed to insecure HTTP connections) in all network communication scenarios.

* + ***Terraform attributes:***
    - Provider Ref: [google\_app\_engine\_standard\_app\_version | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/app_engine_standard_app_version)
    - Provider ref: [google\_app\_engine\_flexible\_app\_version | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/app_engine_flexible_app_version)

***Test cases:***

**Pass cases**

NOTE: In order for a pass to occur, **all** of the requirements **must** be fulfilled:

* + For 'google\_app\_engine\_standard\_app\_version' , the 'security level' argument is set to 'SECURE\_ALWAYS'
  + For 'google\_app\_engine\_flexible\_app\_version' , the 'security level' argument is set to 'SECURE\_ALWAYS'

**Fail case:**

NOTE: If only one, two, or none of the "Pass Cases" are present, policy will consistently result in a fail. The following are some examples of fail cases:

* + For 'google\_app\_engine\_standard\_app\_version' , the 'security level' argument is set to something other than 'SECURE\_ALWAYS'
  + For 'google\_app\_engine\_flexible\_app\_version' , the 'security level' argument is set to something other than 'SECURE\_ALWAYS

4.12 Ensure the Latest Operating System Updates Are Installed on all Virtual Machines in All Projects

***Sentinel Policy Name:***

* + 4.12 Ensure the Latest Operating System Updates Are Installed On Your Virtual Machines in All Projects

***Category :***

* + Google Compute Engine

***Description of Policy:***

* + As per CIS benchmarks, it is recommended to keep an operating system up to date with operating system updates and security patching. This is the best way to secure against ever evolving known vulnerabilities and bugs in programs that can be used in cyber attacks by bad actors.

***Sentinel Policy Restriction:***

* + This policy ensures that the **latest** security /updates patches as well as **critical** operating system updates are installed on all virtual machines for all projects.
  + The **latest** security patches and **critical** operating system updates are deployed to virtual machines in all projects on the **first Tuesday of every month at 12:00 AM EST (midnight)**
  + Optional updates and non- critical patches are optional and can be configured as needed, this policy ensure that the patches and updates with "Critical" or "High priority" association are applied.

***Terraform attributes:***

Provider Ref: [google\_os\_config\_patch\_deployment | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/os_config_patch_deployment)

***Test cases:***

**Pass cases**

NOTE: In order for a pass to occur, **all** of the requirements **must** be fulfilled:

* + For all 'google\_os\_config\_patch\_deployment' resources, the "Instance\_filter.all" must be TRUE. The ensures that **ALL** VMs are included in the patch deployment
  + For all 'google\_os\_config\_patch\_deployment' resources, ensure that 'excludes = null' (or ensure this is not defined in main.tf) This will ensure that all security and OS update packages are included in the patch deployment
  + For all 'google\_os\_config\_patch\_deployment' resources, ensure the 'apt' update type is 'UPGRADE'. This ensure that packages are only updated (older packages are not removed, only updated). This will reduce the potential that a packaged need for an application to run is removed. This is the Patch configuration for Linux VMs: Debian, Ubuntu
  + For all 'google\_os\_config\_patch\_deployment' resources, ensure the 'yum' update has 'security = true' This will ensure all security updates are installed on Linux VMs: RHEL, CentOS
  + For all 'google\_os\_config\_patch\_deployment' resources, ensure the 'zypper' update has 'categories = ["security"]' and 'with\_update = true'. This will ensure that optional security updates are not installed, only the required security updates are installed. Patch configuration for Linux Enterprise servers: SuSE (German-based open-source software firm)
  + For all 'google\_os\_config\_patch\_deployment' resources, ensure the 'windows\_update' update has 'classifications = ["SECURITY", "CRITICAL"]' This will all CRITICAL security updates and CRITICAL operating system updates are installed
  + Other patch configurations are optional, however, the 'main.tf' presents recommended configuration such as 'disruption\_budget' and 'rollout'

**Fail case:**

NOTE: If only one, two, or none of the "Pass Cases" are present, policy will consistently result in a fail. The following are some examples of fail cases:

* + For 'google\_os\_config\_patch\_deployment', the 'Instance\_filter.all' attribute is set to something other than "true"