Continuous Container Visibility and Compliance

Cloud Guard Dome9 for Containers

Gain visibility and continuously ensure compliance in containerized environments

Product Benefits

- Visibility and Visualization
- Security Posture and Compliance
- Governance
- Auto Remediation

Product Features

- Container Inventory
- Traffic Visibility and Investigation with Log.ic
- Compliance for Containers
- CloudBots for Cloud Native Containers
- Continuous Vulnerability Scanning & Assessment

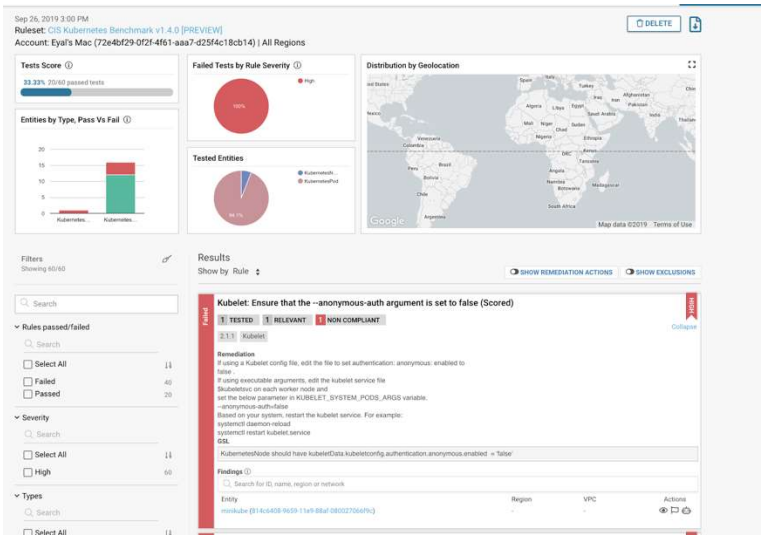
INSIGHTS

Container adoption is on the rise. The first step in securing containers is gaining visibility into the deployment- mainly, what is deployed. Next it is critical to embed security and compliance into the software development process for the security of your applications.

SOLUTION

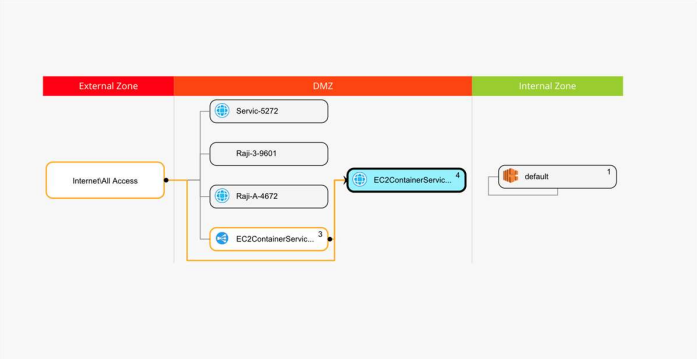
CloudGuard provides a single console view of all your assets, across different platforms, including cloud IAAS, PAAS services, as well as cloud native and customer managed containers.

Using the CloudGuard Dome9 Compliance Engine, you can easily ensure that their configuration is in compliance with known baselines such as CIS Kubernetes Benchmarks or NIST 800-190 for containers regardless of where they are hosted (GCP, AWS, Azure, On-Prem, OpenShift etc).



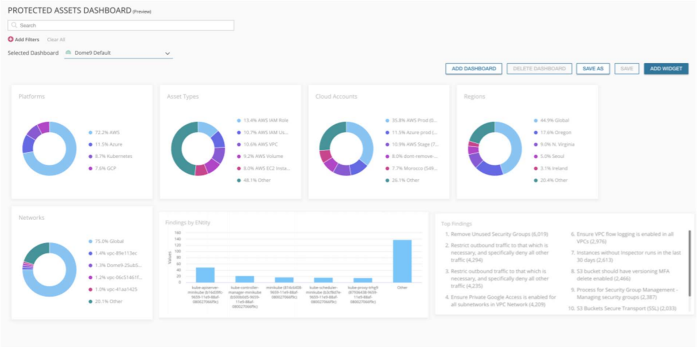
VISIBILITY INTO SECURITY POSTURE

CloudGuard Dome9 provides a powerful visualization of cloud assets, including network topology, firewalls and more for cloud native containers (ECS, GKE and soon AKS)



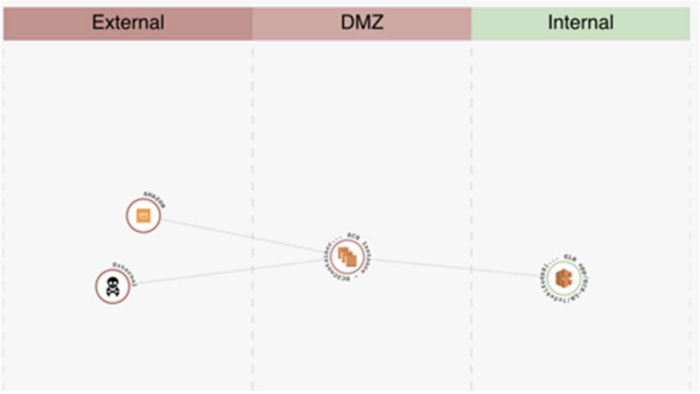
UNIFIED MANAGEMENT, GRANULAR REPORTING

CloudGuard Dome9 presents a single console view of all your assets, on all platforms including native and managed containers, from which you can search or filter for specific assets of interest and see details about their security posture.



TRAFFIC VISIBILITY AND INVESTIGATION

CloudGuard Log.ic takes VPC flow logs and CloudTrail logs from AWS, and enriches the data with the actual service, threat cloud IOC information and other types of enrichment. As part of the supported services, CloudGuard Log.ic shows how the ECS service communicates with other services. It provides the user with the ability to visualize the data flows and run GSL queries for immediate incident response and threat hunting purposes. With CloudGuard Log.ic, you can investigate and identify suspicious ECS related activity—proving investigation and threat analytics capabilities for ECS traffic.



CONTAINERS SECURITY POSTURE AND COMPLIANCE

Cloud Managed Containers Compliance

CloudGuard Dome9 helps identifying misconfigured containers by evaluating security settings of cloud managed containers including ECS, GKE and soon AKS. The user will be able to run compliance rules on the configuration in order to enforce policies, including allowed flows in the cluster, which service is open to the internet, which is internal, alert on mis-configured containers and vulnerabilities such as runC, titled CVE-2019-5736).

The CIS benchmark for GCP, features a new section around Google Kubernetes Engine (GKE) along with other foundational cloud security areas: identity and access management, logging and monitoring, networking, storage, databases and virtual machines

Dome9 supports all the compliance requirements listed in CIS benchmarks for Google:
https://www.cisecurity.org/benchmark/google_cloud_computing_platform/

Continuous Vulnerability Scanning

CloudGuard Workload provides continuous scanning of container environment during runtime. Through AI and machine learning, CloudGuard Workload provides automated protection to intuitively secure container workloads during runtime, and continuously scans environment to ensure it maintains compliance with external and custom policies. This added security prevents threats during runtime without comprising application

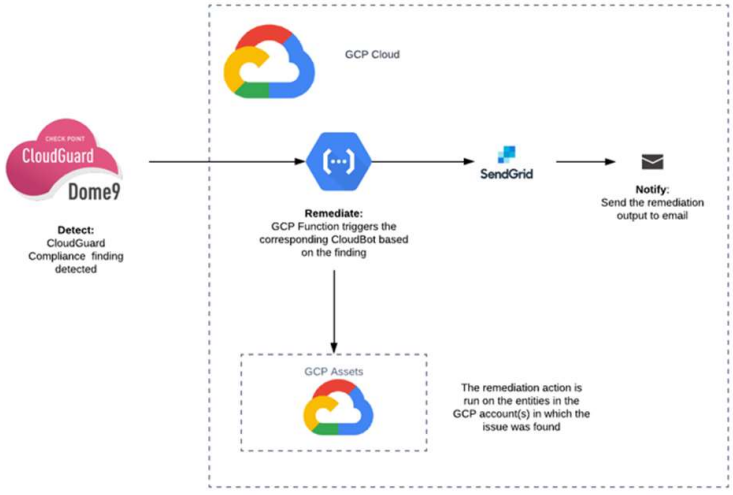
Auto-Remediation - CloudBots for GKE

CloudBots is an open-source project on GitHub that provides the agility needed to keep up with the pace of securing dynamic cloud applications.

The CloudBots technology is developed by the CloudGuard Dome9 team for autoremediation and continuous compliance for cloud environments.

The bots are triggered by findings identified by Dome9's Continuous Compliance engine.

The remediation platform is deployed within your cloud account on AWS, using Lambda; subscription on Azure, using Azure Function; or project in GCP, using cloud functions. CloudBots do not require providing Dome9 write permissions to your cloud environment – you can continue using Dome9 in
a read-only mode.



Customer Managed Clusters- Compliance

CloudGuard Dome9 now supports CIS Kubernetes Benchmark
The CIS Kubernetes Benchmark consists of over a hundred of specific recommendations for containers security. Each requirement of CIS Benchmark includes control requirements and remediation steps. Dome9 supports over 50% of CIS Kubernetes Benchmark - V1.4.0 requirements as of today and continuously increasing this coverage to fully automate compliance efforts of our clients.