

Dome9 Security

THE LEADING CLOUD INFRASTRUCTURE SECURITY PLATFORM



First Last

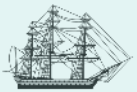
email@dome9.com

Dome9 Security



About Dome9

Innovative SaaS Platform for Everything Public Cloud Infrastructure Security



Vanguard



CITRIX

apigee

AON

cadence

CAR AND DRIVER

250+ enterprise customers



Founded in 2011



Strong leadership:
Check Point, HP, Nutanix & IDF



HQ in Mountain View, CA with
R&D in Tel Aviv; 40+ employees



Patents awarded and filed for cloud
security orchestration technologies

Partners:



Google Cloud Platform



About Dome9

Cloud Native Platform for Everything Public Cloud & Infrastructure Security

- SaaS based
 - Agentless
 - 5 minute setup (actually!)
 - Completely focused on the public cloud
- What we do:
 - Infrastructure security
 - Visibility across accounts and clouds
 - What we don't do:
 - Host / agent based security
 - IDS / IPS

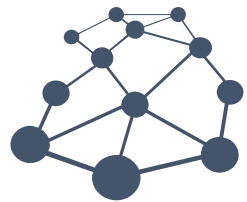
Partners:



Comprehensive Cloud Security Starts With Dome9



Innovative SaaS platform for security and compliance across public cloud environments



**Network
Security**




**Compliance &
Governance**



**Enhanced IAM
Protection**



Dome9 Clarity: Powerful Network Visualizations

 Protect Network Security IAM Safety Dynamic Access Clarity Compliance & Governance Users & Roles

166 alex+demo@dome9.co...

Clarity Home / AWS Prod / Oregon / Main Demo VPC / default

COMPACT LANDSCAPE HIDE EMPTY SG PEERED VPCS VPC FLOW LOGS PRINT SEARCH FILTER BY TAGS Main Demo VPC (vpc-89e113ec) SECURITY GROUPS

External Zone

DMZ

Partially Open

Effectively Internal

Internal Zone

Internet/All Access

194.90.1.5/32

NYC Office

Monitor External B...

Partner extranet s...

My rackspace serve...

Trusted Office IP ...

default 1

LB-Web 1

Common SG 6

monitoring 2

App2_ApplicationSe...

WebServers 2

Application-Load-B...

Web Monitor 1

Lambda-SG 1

App2_Web

App1 Servers 1

App2_DB

MQ 1

DB servers 3

DMZ

default sg-bc1ea9d9 Open in central

Instance (1) DB1

Rules (2) TCP 21 FTP TCP 22 SSH

Sources (2) Web Monitor 0.0.0.0/0

Targets (1) WebServers

Tags application app123

I-C94ED8C4 Search logs SEARCH ALL REJECTED ACCEPTED LAST 30 MIN UTC LOCAL EXPORT TO CSV

Source	Source Port	Destination	Dest Port	Protocol	Packets	Bytes	Time	Action
95.215.1.37	49705	DB1	3501	TCP	1	40	Aug 28th 2017, 08:04:25 pm	REJECT
93.174.93.136	54231	DB1	1989	TCP	1	40	Aug 28th 2017, 08:23:04 pm	REJECT
92.24.157.83	14908	DB1	23	TCP	1	40	Aug 28th 2017, 08:24:54 pm	REJECT
91.211.0.109	51865	DB1	3387	TCP	1	40	Aug 28th 2017, 08:20:18 pm	REJECT
91.211.0.104	57634	DB1	3390	TCP	1	40	Aug 28th 2017, 08:04:25 pm	REJECT
82.80.217.70	54475	DB1	445	TCP	1	48	Aug 28th 2017, 08:12:16 pm	REJECT

Clarity helps you visualize Security Group configurations, exposure to the public internet, and VPC Flow Logs all from one central view



Dome9 Compliance Engine: Cloud Audit Better and Much Faster

The Compliance Engine and GSL rule language allows you to run assessments against known security frameworks and your own custom best practices

Dome9 Protect Network Security IAM Safety Dynamic Access Clarity Compliance & Governance Users & Roles

Compliance Engine Policies Dashboard Assessment History Playground Aug 28, PCI-DSS

Text Editor Rule Builder

Rule GSL ?

Instance where tags with [key='hasPCI' and value='true'] should have image='ami-aa5ebdd2'

AWS

ApplicationLoadBalancer CloudTrail EFS ELB IAM IAMGroup IAMRole IAMUser Instance KMS Lambda NACL RDS Redshift Region S3Bucket SecurityGroup Subnet VPC

Azure

NetworkSecurityGroup VirtualMachine

Google

Network Subnet VMInstance

Test Rule

Account Region VPC

AWS Prod ALL ALL

TEST

Dome9 Protect Network Security IAM Safety Dynamic Access Clarity Compliance & Governance Users & Roles

Compliance Engine Policies Dashboard Assessment History Playground Aug 28, PCI-DSS

Aug 28, 2017 1:26 PM
PCI-DSS
Automated Validation of PCI-DSS Security Control Mapping Validations, https://s3.amazonaws.com/quickstart-reference/enterprise-accelerator/pci/latest/assets/PCI-DSS-Security-Controls-Mapping.xlsx

DELETE PRINT

AWS Prod All Regions 76 Total

27.63% Passed (21)

72.37% Failed (55)

0% Error

Entities by type, Pass Vs Fail

Failure by Severity

Map

Tested Entities

Filters

Showing 76/76 CLEAR

Results

Failed (55)

Passed (21)

Severity

High (67)

Low (8)

id: "string"

type: "string"

name: "string"

dome9Id: "string"

accountNumber: "string"

region: "string"

source: "string"

tags: Array [1]

vpc: Object

Results

SHOW GSL

FAILED Ensure VPC Flow Logging is Enabled in all Applicable Regions

14 TESTED 12 RELEVANT 9 NON COMPLYING

PCI-DSS Section 1.1.1 PCI-DSS Section 10.5.*

FAILED Process for Security Group Management - Detection of new Security Groups

14 TESTED 14 RELEVANT 12 NON COMPLYING

PCI-DSS Section 1.1.1

ED Ensure no security groups allow ingress from 0.0.0.0/0 to RDP (TCP:3389)



Protect Against Compromised Credentials and Identity Theft

The screenshot displays the Dome9 IAM Safety console. The top navigation bar includes links for Protect, Network Security, IAM Safety (active), Dynamic Access, Clarity, Analysis, and Users & Roles. The main header shows 'IAM Safety - Console Hardening' with a search bar and an '+ ADD CLOUD ACCOUNT' button. Below this, a table lists cloud accounts with columns for Account Name, Status, Active, Pending, IAM Users, and IAM Roles. The 'AWS Prod' account is highlighted, showing it is 'Enabled' with 9 active and 4 pending users. A legend indicates green for 'Protected' and red for 'Not Protected'. A mobile device screen shows an 'IAM Safety authorization window opened for AWS Prod'. On the right, a detailed view for the 'AWS Prod' account (ID: 086071956115) shows tabs for Dome9 Users, IAM Users, and IAM Roles. The 'IAM Users' tab is active, displaying a list of users with columns for User Name, IAM Entity, Status, and actions. The list includes users like adam.neale@eb2bcom.com, amit+demo@dome9.com, and others, with status indicators for 'Not Invited', 'Enabled', 'Disabled', and 'Pending'. Action buttons like 'INVITE USER', 'UNPROTECT', 'REPROTECT', and 'DISASSOCIATE' are available for each user.

Account Name	Status	Active	Pending	IAM Users	IAM Roles
AWS Prod	Enabled	9	4		

User Name	IAM Entity	Status	Actions
adam.neale@eb2bcom.com		Not Invited	INVITE USER
amit+demo@dome9.com	amit_demo	Enabled	UNPROTECT
andrew.sciberras+dome9@eb2bcom.com		Not Invited	INVITE USER
arik.blumin+dome9@eb2bcom.com		Not Invited	INVITE USER
arik.blumin+perm@dome9.com	splunk_user	Disabled	REPROTECT, DISASSOCIATE
assaf+demo@dome9.com	Assaf_Demo	Enabled	UNPROTECT
awssummit@dome9.com	harish	Enabled (Deleted)	UNPROTECT
calvin.yeo+dome9@eb2bcom.com		Not Invited	INVITE USER
chen+demo@dome9.com		Not Invited	INVITE USER
chuck+auditor@dome9.com		Not Invited	INVITE USER
chuck+demo@dome9.com		Pending	CANCEL INVITATION
corin@dome9.com		Pending	CANCEL INVITATION

IAM Safety

Like a 'sudo for AWS' - privilege elevation on an as-needed basis for protected actions with second-level out-of-band authorization from a mobile device for critical updates.

Thank you!



www.dome9.com