FireMon Cloud Defense

Asset Manager offers FireMon's Cloud Defense (formerly called DisruptOps (branding name are being updated)) integration, which replaces the former CloudVisibility engine.

Cloud Defense is a cloud security operations platform to monitor, alert and respond to security risk across your public cloud infrastructure.

Prerequisite

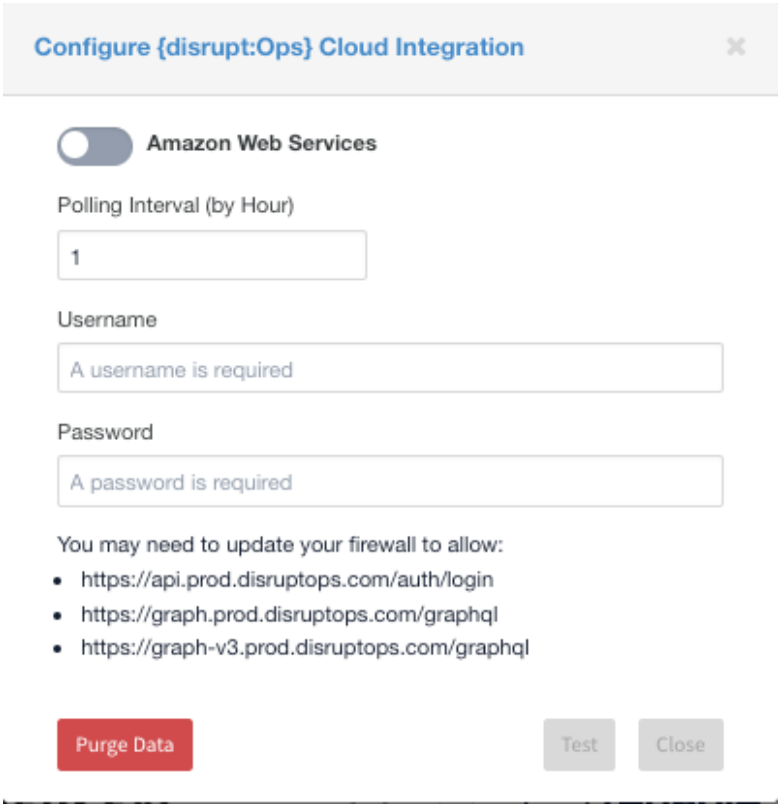
To use the feature, you must have the Cloud Defense platform deployed in your AWS environment. For guidance, open a Support ticket and request "Disrupt:Ops".

FireMon Support will respond by providing you with implementation steps and login credentials.

They will also help you deploy the necessary "*cloudformation* stack."

Configuration

1. To configure this new integration, browse to **Settings** > **Integrations** > **Disrupt:Ops** and click **Configure.**
2. Complete the form, entering your Disrupt:Ops credentials in the **Username** and **Password** fields (*not* your AWS credentials).



3. Firewall ACL rules must be open for Asset Manager to access these URLs over port 443
    a. https://api.prod.disruptops.com/auth/login
    b. https://graph.prod.disruptops.com/graphql
    c. https://graph-v3.prod.disruptops.com/graphql

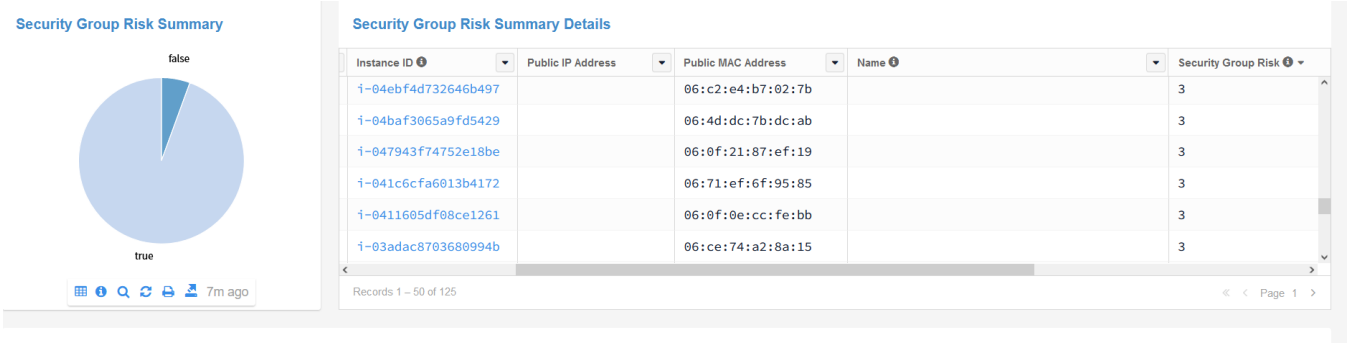
DisruptOps Cloud Dashboard

Navigate to **Dashboards** > **Integrations** and view your results under the **DisruptOps Cloud Dashboard**.

Security Group Risk

Asset Manager considers the following factors in calculating the Security Group violation:

1. Wildcard in a Security Group.
2. IPv4 mask is too large for a Security Group.
3. Src/Dest checks disabled on an instance
4. Inbound/outbound path to the public internet (direct and indirect)

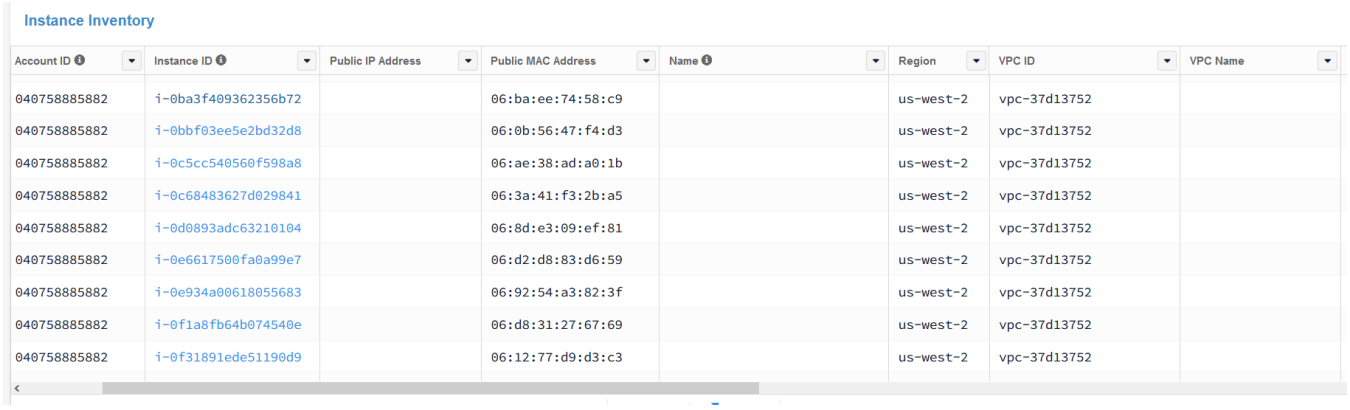


Instance Inventory

This widget will display AWS Instance Information including:

1. Instance ID
2. Public MAC Address
3. Public IP
4. VPC information
5. Security Group information
6. Region

All this information can be configured into reports; combing you cloud instance information with your on-prem devices.



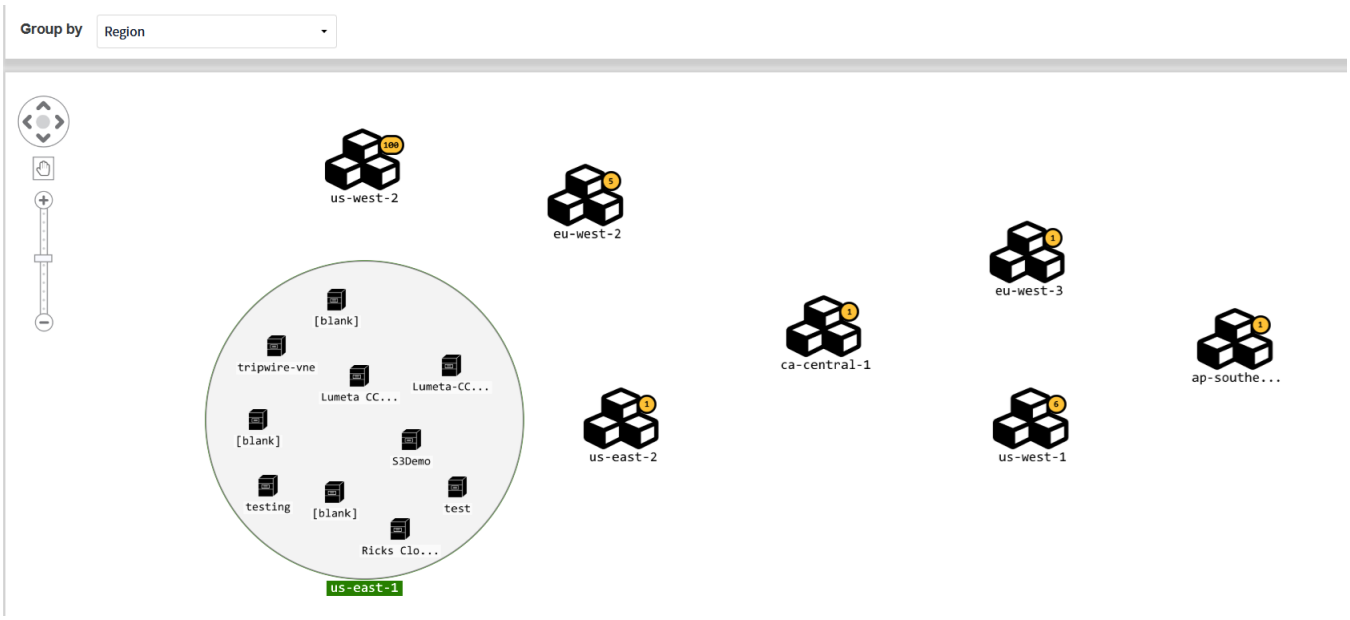
Map

The Cloud Map offers a quick view of your AWS instances.

The map can be grouped by:

- Provider
- Account
- Region
- VPC ID

The Map will only show information for which we have retrieved EC2 Instances.


Group by
Region
100
us-west-2
5
eu-west-2
1
eu-west-3
1
ca-central-1
1
ap-southe...
1
us-east-2
6
us-west-1
[blank]
tripwire-vne
Lumeta CC...
Lumeta-CC...
[blank]
S3Demo
testing
[blank]
test
Ricks Clo...
us-east-1