

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).

Configure {disrupt:Ops} Cloud Integration

Amazon Web Services

Polling Interval (by Hour)

1

Username

A username is required

Password

A password is required

You may need to update your firewall to allow:

- <https://api.prod.disruptops.com/auth/login>
- <https://graph.prod.disruptops.com/graphql>
- <https://graph-v3.prod.disruptops.com/graphql>

Purge Data

Test

Close

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

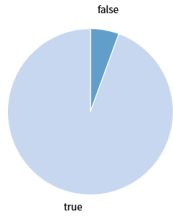
Navigate to **Dashboards > Integrations** and view your results under the **DisruptOps Cloud Dashboard**.

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)

Security Group Risk Summary



Security Group Risk Summary Details

Instance ID	Public IP Address	Public MAC Address	Name	Security Group Risk
i-04ebf4d732646b497		06:c2:e4:b7:02:7b		3
i-04baf3065a9fd5429		06:4d:dc:7b:dc:ab		3
i-047943f74752e18be		06:0f:21:87:ef:19		3
i-041c6cfa013b4172		06:71:ef:6f:95:85		3
i-0411605df08ce1261		06:0f:0e:cc:fe:bb		3
i-03adac8703680994b		06:ce:74:a2:8a:15		3

Records 1 – 50 of 125

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.

Instance Inventory

Account ID	Instance ID	Public IP Address	Public MAC Address	Name	Region	VPC ID	VPC Name
040758885882	i-0ba3f409362356b72		06:ba:ee:74:58:c9		us-west-2	vpc-37d13752	
040758885882	i-0bbf03ee5e2bd32d8		06:0b:56:47:f4:d3		us-west-2	vpc-37d13752	
040758885882	i-0c5cc540560f598a8		06:ae:38:ad:a0:1b		us-west-2	vpc-37d13752	
040758885882	i-0c68483627d029841		06:3a:41:f3:2b:a5		us-west-2	vpc-37d13752	
040758885882	i-0d0893adc63210104		06:8d:e3:09:ef:81		us-west-2	vpc-37d13752	
040758885882	i-0e6617500fa0a99e7		06:d2:d8:83:d6:59		us-west-2	vpc-37d13752	
040758885882	i-0e934a00618055683		06:92:54:a3:82:3f		us-west-2	vpc-37d13752	
040758885882	i-0f1a8fb64b074540e		06:d8:31:27:67:69		us-west-2	vpc-37d13752	
040758885882	i-0f31891ede51190d9		06:12:77:d9:d3:c3		us-west-2	vpc-37d13752	

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

