Cloud Visibility Reports

Reports provide valuable statistical information that you can use as insights to the network and its general health, and decide accordingly. Multicloud Defense enables you to generate the following reports:

Discovery

The Generate a Discovery Report is generated by taking out-of-band traffic information from DNS queries and VPC flow logs, and correlating the data with threat intelligence and cloud inventory information. These logs are only available if you configure the VPC of your cloud service provider to send logs to an S3 bucket. These logs are then transferred directly to the Multicloud Defense Controller.

The report contains:

- **Top of Discovery Report** - Network and cloud asset analytics, presented in volume and distinct counts of field values. You can derive insights on what is happening in your cloud environment by quantifying network behavior.
- **Network Traffic – Bytes** - This graph displays the volume of bytes by traffic direction. You can view where the volume of bytes is going - Ingress, Egress, or East-West.
- **Network Traffic – Packets** - This graph displays the volume of packets by traffic direction. You can view where the volume of packets is going - Ingress, Egress, or East-West.
- **Network Traffic – Events** - This graph displays the volume of events by traffic direction. You can view where the volume of events is going - Ingress, Egress, or East-West.
- **Ingress Account Summary** - This summary displays the distinct count of cloud assets with ingress network traffic, by CSP. You can view review the flow of assets communicating into a CSP environment.
- **Egress Account Summary** - This summary displays the distinct count of cloud assets with egress network traffic, by Cloud Service Provider (CSP). You can view review the flow of assets communicating out of a CSP environment.
- **Ingress Network Events by Country** - This geographic heatmap shows the volume of ingress traffic by country. You can view countries that communicate with the cloud environments.
- **Egress Network Events by Country** - This geographic heatmap shows the volume of egress traffic by country. You can view countries that communicate with the cloud environments.
- **Top 10 Source Countries** - This graph displays the top 10 source countries by volume of events, with other network analytics. This is a summary of the top source countries that the cloud environment is communicating with.

- **Top 10 Destination Countries** - This graph displays the top 10 destination countries by volume of events, with other network analytics. This is a summary of the top destination countries that the cloud environment is communicating with.
- **Top 10 Ingress Source IP Addresses** - This graph displays the top 10 source IP addresses by volume, with other network analytics. You can view the entities that create the most inbound events.
- **Top 10 Egress Destination IP Addresses** - This graph displays the top 10 destination IP addresses by volume, with other network analytics. You can view entities that the cloud environment mostly communicates with.
- **Top 10 FQDN Category Names by Volume** - This graph displays the category names by volume for FQDNs. You can view the top category types based on the FQDNs being requested by the cloud environment.
- **Top 10 FQDNs by Volume** - This graph displays the top 10 FQDNs by volume. You can view the top FQDNs that are requested by the cloud environment.
- **Top 10 Malicious FQDNs by Volume** - This graph displays the top 10 malicious FQDNs by volume. If a malicious or suspicious category name is found, the top FQDNs in that category name is displayed here.
- **FQDN Category Name Mapped to MITRE ATT&CK** - This graph displays the top 10 malicious category names mapped to MITRE ATT&CK. This view provides more context on how the FQDN category name relates to an attack chain by using the Enterprise MITRE ATT&CK framework.

Threat Indicators Snapshot

The Generate a Threat And Cloud Analytics Report report is a compilation of data on the gateway instance. You can use this report to determine the gateway's endurance under duress by examining traffic patterns, when and how thresholds are met, trends of attacks, and specific instances. The report includes the following points:

- **IDS/IPS Detection** - This data shows how many attacks are detected, the type of attack, the time of the detected attacks, and the top ten IDS/IPS signatures over the time range selected.
- **WAF Detection** - This data shows how many attacks are detected by WAF rules, the time of the detected attacks, and the top ten WAF signatures over the time range selected.
- **Relocation of Threats by Volume** - This choropleth map shows the volume of attacks for both WAF and IDS/IPS events by country in volume.
- **Top Ten Attacking Countries by Volume and Time** - This horizontal bar chart depicts the volume of the top 10 countries that during the entirety of the timespan produced the most events, then displayed breaking that volume across the time increments for which the events occurred during the timespan.
- **Policy and Prevention** - This data chart shows the action that is taken by the gateway security type in whichever CSP environment it is deployed in. This includes the type of action, how many events generated from the action, the gateway security type and more.

You **must** have Web Application Firewall (WAF), intrusion detection and prevention (IDS/IPS) rules that are enabled in your policy for the Multicloud Defense Gateway to collect and poll data.

For Additional Information:

- Generate a Discovery Report, on page 3

• Generate a Threat And Cloud Analytics Report, on page 3

Generate a Discovery Report

A discovery report is generated by taking DNS queries and VPC flow logs that have been sent to an S3 bucket prior to getting processed by the Multicloud Defense Controller.

Procedure

Step 1 In the Multicloud Defense Controller page, navigate to **Report**.

Step 2 Select **Discovery**.

Step 3 Under Threat & Cloud Analytics Report, select the **Frequency** from the drop-down list for the data that is pulled: daily, weekly, monthly, quarterly, or yearly.

- **Daily** - From 12 a.m. for 24 hours. This is in UTC time.
- **Weekly** - From Monday to Sunday.
- **Monthly** - Generally from the beginning to the end of the month.
- **Quarterly** - From the beginning to end of a quart. Quarters are generally defined as from January 1 - March 31, April 1 - June 30, July 1 - September 30, and October 1 - December 31.
- **Yearly** - From January 1 to December 31 of the year selected.

Step 4 Select a date. Use the drop-down **Calendar** to select the time range or specific days that you want to collect data on. Days that are grayed out have no data to compile. If you have no data available to generate a report, confirm your policies contain WAF and IDS/IPS rules.

Step 5 Click **Generate Report**. The Discovery Report is generated in a new tab.

Step 6 To save the report locally, click **Print Report**. Navigate to a location on your local server and save the report.

Generate a Threat And Cloud Analytics Report

The Threat and Cloud Analytics Report is a **Threat Indicator Snapshot** that is generated by using the traffic collected and inspected by Multicloud Defense Gateway. This provides a more comprehensive report as Multicloud Defense is now in the datapath and compliments the discovery report.

Note that reports cannot be generated for the day of, since a qualitative summarization of events cannot be made until end of day, end of month, end of quarter, or end of year.

Note You **must** have Web Application Firewall (WAF), intrusion detection and protection (IDS/IPS) rules enabled in your policy in order for the Multicloud Defense Gateway to collect and poll data. For more information, see the following links respecitvely:

- Web Application Firewall
- Network Intrusion (IDS/IPS) Profile

Use the following procedure to generate a Threat And Cloud Analytics with the threat indicators snapshot:

Procedure

Step 1 In the Multicloud Defense Controller page, navigate to **Report**.

Step 2 Select **Threat Indicators Snapshot**.

Step 3 Under Threat & Cloud Analytics Report, select the **Frequency** from the drop-down list for the data that is pulled: daily, weekly, monthly, quarterly, or yearly.

- **Daily** - From 12 AM for 24 hours. This is in UTC time.
- **Weekly** - From Monday to Sunday.
- **Monthly** - Generally from the beginning to the end of the month.
- **Quarterly** - From the beginning to end of a quart. Quarters are generally defined as from January 1 - March 31, April 1 - June 30, July 1 - September 30, and October 1 - December 31.
- **Yearly** - From January 1 to December 31 of the year selected.

Step 4 Select a date. Use the drop-down **Calendar** to select the time range or specific days that you want to collect data on. Days that are grayed out have no data to compile. If you have no data available to generate a report, confirm your policies contain WAF and IDS/IPS rules.

Step 5 Click **Generate Report**.

Step 6 The report is generated. To save the report locally, click **Print Report**. Navigate to a location on your local server and save the report.