Using RiskVision to Investigate Cloud App Use

Many organizations have moved to cloud-based applications for a variety of core business functions, such as customer relationship management, human resources, and online collaboration.

Individuals, also, are using a variety of cloud apps for social networking, personal data storage, streaming media, and so on.

With its Cloud Apps Plugin, powered by Imperva® Skyfence, RiskVision can help you:

- Understand which cloud apps your users are accessing.
- Assess the risk that cloud app use may pose to your organization.

In addition, when RiskVision monitors traffic after it has passed through an SSL decryption product, the Cloud Apps Plugin can work in conjunction with other analysis tools to detect data loss and malicious activity.

For help investigating cloud app incidents, see:

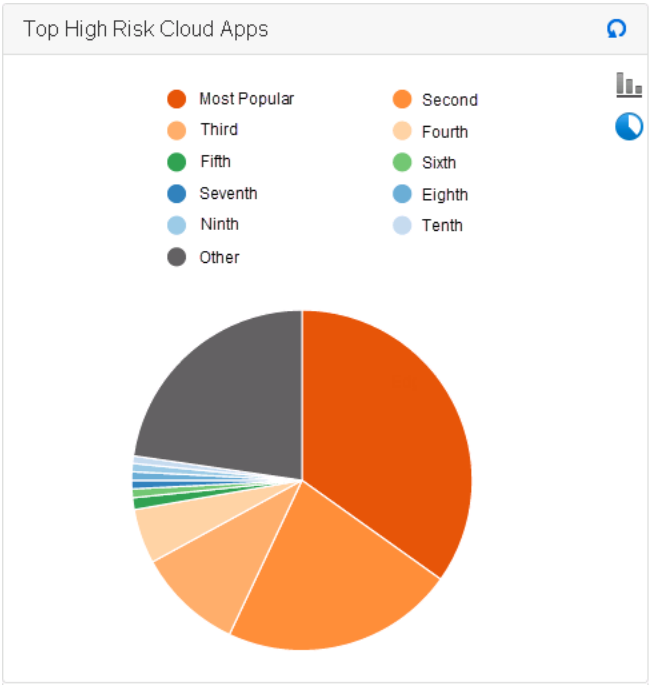
- *Which high-risk cloud apps are being accessed most frequently in my network?*
- *Which users are accessing high-risk cloud apps most frequently?*
- *Are there data loss or data theft incidents associated with cloud app access?*
- *How do I find incidents associated with a specific cloud app?*
- *How can I find out which cloud apps are associated with incidents in my network?*

For more information about the cloud app details available with RiskVision, see *Understanding the results of cloud app analysis*.

Which high-risk cloud apps are being accessed most frequently in my network?

Investigate Cloud App Use | TRITON RiskVision | 01-June-2016

Use the dashboard charts on the **Reporting > Cloud Apps** page to get a quick overview of the most popular high-risk cloud apps that users at your organization are accessing.



By default, the **Top High Risk Cloud Apps** chart shows up to the top 10 most-accessed, high-risk cloud apps.

- Use the toggle buttons to the right of the chart to change from pie to bar chart view.
- Position the mouse over a pie slice or bar to see the cloud app name and the amount of bandwidth consumed by transactions that app.

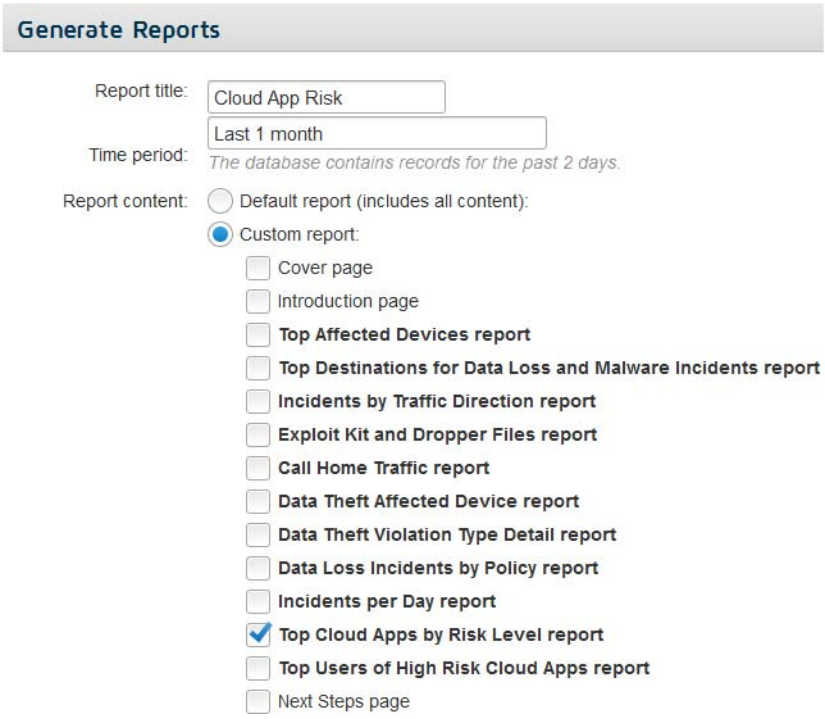
New cloud app incidents are shown in the Transaction Viewer in real time, and aggregated to update the chart every 6 hours.

To further investigate use of a specific app, see *How do I find incidents associated with a specific cloud app?*.

More information about potentially risky cloud apps is available in the **Top Cloud Apps By Risk Level** presentation report. To generate the report:

1. Navigate to the **Reporting > Executive Reports** tab.
2. Enter a descriptive **Report title** and select the **Time period** to include in the report.

3. Select the **Custom report** radio button, then select **Top Cloud Apps by Risk Level**.



4. Indicate how many records to include via the **Top N number** field (10, by default), then select a **Report format**.
5. To see information about cloud app transactions that did not have associated malware or data loss incidents:
   - Version 2.1: Mark the check box next to **Show hidden incidents**.
   - Version 2.0: Clear the check box next to **Hide suppressed incidents**.
6. Click **Run Report Now**.
7. When the report has generated, click the link below the Run Report Now button to review the report.

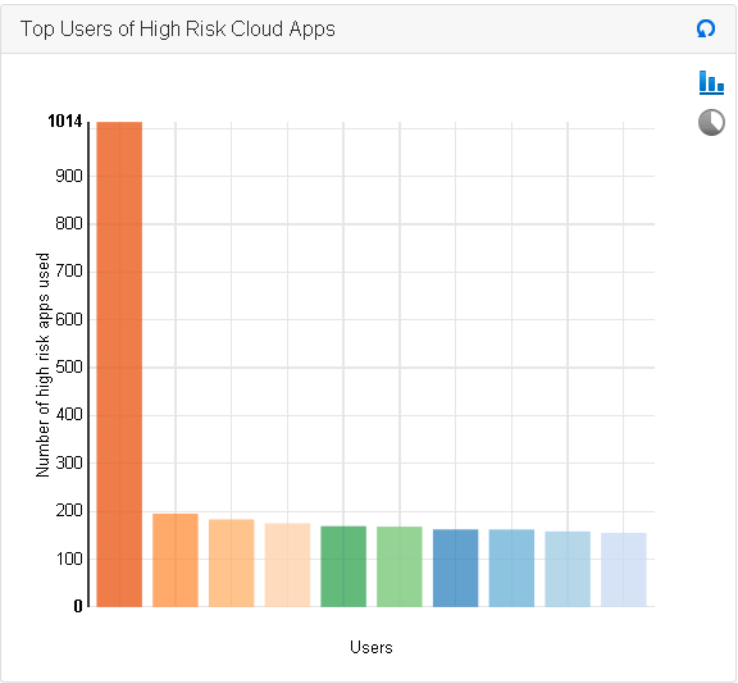
   The report includes 2 sections:

   - A summary report that lists the most-used cloud apps by risk level, with the number of users accessing each and the amount of bandwidth used
   - A detail report showing the app name, URL, total (upstream and downstream) bandwidth use, and last seen date, as well as a description of the app.

Which users are accessing high-risk cloud apps most frequently?

Investigate Cloud App Use | TRITON RiskVision | 01-June-2016

Use the dashboard charts on the **Reporting > Cloud Apps** page to get a quick overview of the users accessing high-risk cloud apps most often.



By default, the **Top Users of High Risk Cloud Apps** chart shows the users who have accessed high-risk cloud apps most frequently, based on number of visits to the apps. Users may be identified by IP address or, if RiskVision is receiving X-Authenticated-User headers, user name.

- Use the toggle buttons to the right of the chart to change from bar to pie chart view.
- Hover the mouse over any bar or pie slice in the chart to see the number of high risk cloud apps that the user visited.

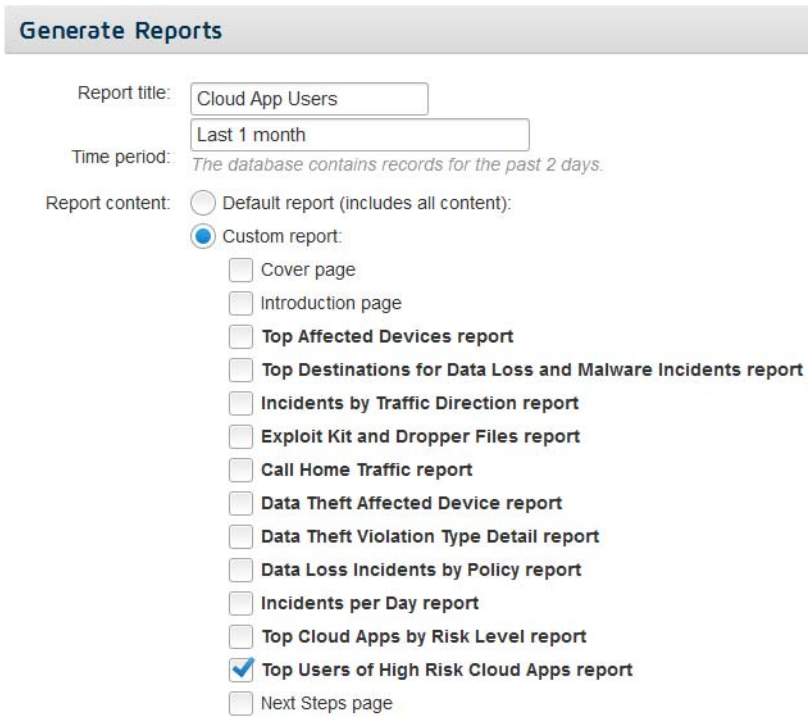
New cloud app incidents are shown in the Transaction Viewer in real time, and aggregated to update the chart every 6 hours.

Use the Transaction Viewer to find out more about activity from a specific user.

More information about users of high risk cloud apps with the **Top Users of High Risk Cloud Apps** presentation report. To generate the report:

1. Navigate to the **Reporting > Executive Reports** tab.
2. Enter a descriptive **Report title** and select the **Time period** to include in the report.

3. Select the **Custom report** radio button, then select **Top Users of High Risk Cloud Apps**.



4. Indicate how many records to include via the **Top N number** field (10, by default), then select a **Report format**.
5. To see information about cloud app transactions that did not have associated malware or data loss incidents, clear the check box next to **Hide suppressed incidents**.
6. Click **Run Report Now**.
7. When the report has generated, click the link below the Run Report Now button to review the report.

   The report includes 2 sections:

   - A summary report that lists the users who connected to the most cloud apps, with the number of monitored apps accessed at each risk level (high, medium, low).
   - A report listing each user who accessed one or more high-risk cloud apps, with the name of the app or apps that each used.

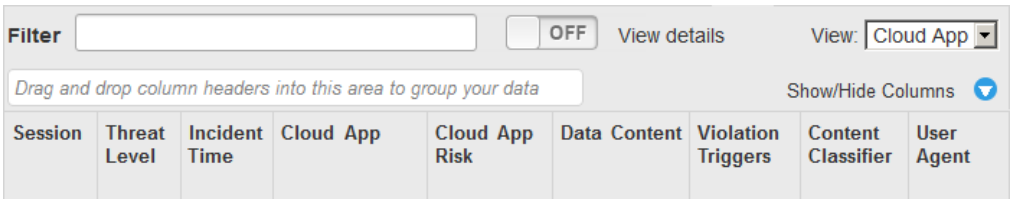
Are there data loss or data theft incidents associated with cloud app access?

Investigate Cloud App Use | TRITON RiskVision | 01-June-2016

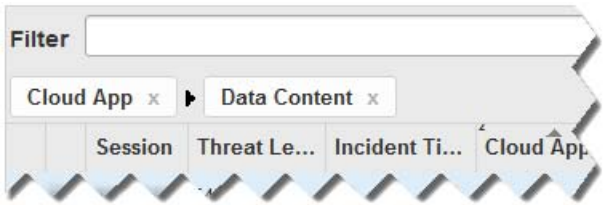
Most user connections to cloud apps are encrypted. In order for RiskVision to detect data loss or data theft incidents in cloud app transactions, it must be configured to monitor traffic that has first passed through an SSL decryption product (like an F5 or A10 appliance).

If RiskVision is monitoring already-decrypted transactions, use the Transaction Viewer on the **Incidents** page in the RiskVision Local Manager to find out if Data Analysis has found data loss or data theft incidents associated with cloud app use.

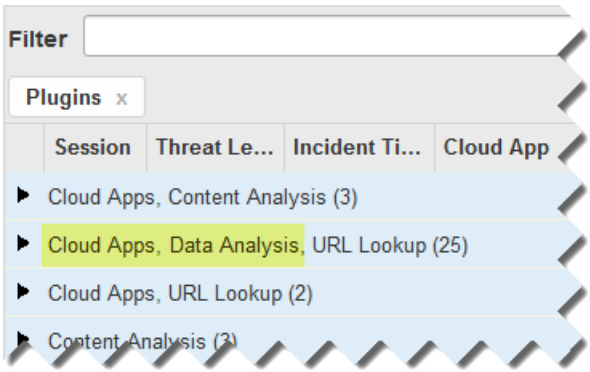
By default, when you select the **Cloud App** option from the View drop-down list, the table includes columns for cloud app name and risk level, and for data analysis content, violation triggers, and content classifiers (or rules).



To look for correlations, try grouping by **Cloud App** and **Data Content**.



You can also try grouping data by **Plugins** to find incidents with results returned by both **Cloud Apps** and **Data Analysis**.

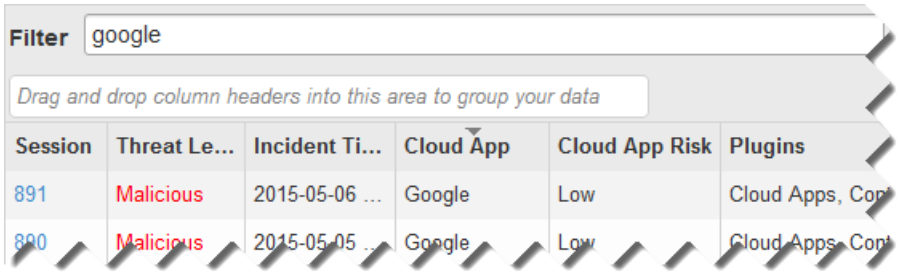


How do I find incidents associated with a specific cloud app?

Investigate Cloud App Use | TRITON RiskVision | 01-June-2016

To find out if users are accessing a specific cloud app, or to look for correlations between a cloud app and security incidents:

1. Go to the **Incidents** page in RiskVision Local Manager.
2. Mark the **Show hidden incidents** check box near the top of the page (next to Time period selector).
3. Click **Refresh**.
4. Select **Cloud App** from the **View** drop-down list to make sure all available data related to cloud app analysis is displayed in the table.
5. In the **Filter** box above the table, enter the name of the cloud app.



Depending on the cloud app name, you may see some non-applicable results. If this occurs, try grouping the results by the Cloud App column.

To do this, click on the **Cloud App** column header in the table and drag the mouse upward slightly (toward the "Drag and drop column headers" box). When you release the mouse, data in the table is grouped and resorted.

How can I find out which cloud apps are associated with incidents in my network?

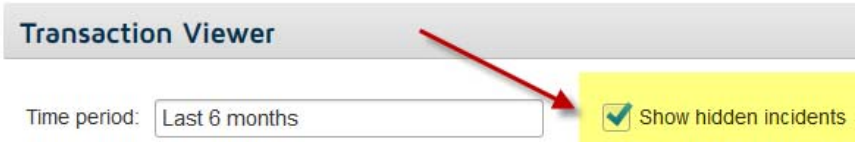
Investigate Cloud App Use | TRITON RiskVision | 01-June-2016

To find out if users are accessing potentially risky cloud apps in your network, or using cloud apps in association with security or data loss incidents:

1. Log in to the RiskVision Local Manager.

   The Incidents page appears, showing the Transaction Viewer.

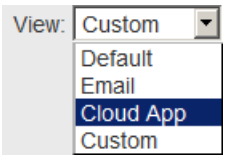
2. Mark the **Show hidden incidents** check box near the top of the page (next to Time period selector).



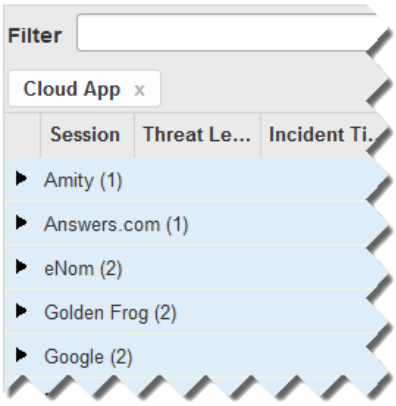
   See *Understanding the results of cloud app analysis*, page 10, for more information about why this step is necessary.

3. Click **Refresh**.

4. Select **Cloud App** from the **View** drop-down list to change the columns shown in the Transaction Viewer table.



5. Click on the **Cloud App** column header in the table and drag the mouse upward slightly (toward the “Drag and drop column headers” box), then release the mouse.



This groups the table by individual cloud apps, giving you an overview of which apps are being used (and most frequently used) in your network.

6. Repeat step 5 for the **Cloud App Risk** column header to see the risk level associated with each app.

   To group by risk level first, then app name, simply drag the **Cloud App Risk** box to the left to adjust the grouping order.

Understanding the results of cloud app analysis

When a transaction is analyzed, the Cloud Apps Plugin:

1. Identifies transactions that include communication with a known cloud app (like Salesforce or Dropbox)

   This identification takes into account both the URL and the IP address of the site that was accessed.
2. Reports the risk level (from low to high) associated with the cloud app

   The risk level is based on several risk factors, described in *What risk factors does cloud app analysis look for?*, page 11.
3. If the risk level associated with the app is high enough, reports a threat score

   The threat score is used in conjunction with results from other plugins to assign an overall threat level (suspicious, malicious) to the incident.

If the Cloud Apps Plugin returns a threat score that exceeds a minimum threshold, the transaction is flagged as an incident and recorded.

- If no malware activity or data loss was found, the incident does **not** appear in the Transaction Viewer by default.

  Mark **Show hidden incidents** to see these records.
- If both cloud app analysis and another type of analysis determine that an incident occurred, the incident **is** displayed in the Transaction Viewer by default.

Information about low risk cloud apps (those below the threshold for creating an incident) appears in the Transaction Viewer only when both of the following are true:

1. An incident is created based on, for example, content analysis or data analysis.
2. The transaction includes communication with a known cloud app that is classified as low risk.

Only the cloud app name (shown in the Cloud App column) and risk level (Shown in the Cloud App Risk column) are displayed in the Transaction Viewer table, but additional information is available in the Details pane. See *How do I find out more about the cloud app associated with an incident?*, page 10, for more information.

How do I find out more about the cloud app associated with an incident?

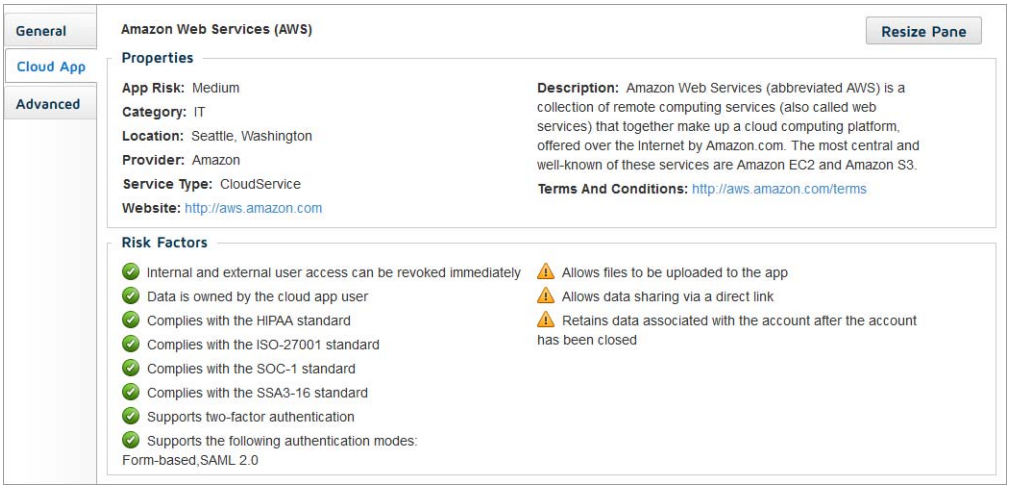
To find more information about the cloud app associated with an incident, and to find out more about the risk level assigned to the cloud app:

1. Select an incident in the Transaction Viewer that includes cloud app data.

2. Click **View Details**.
3. In the Details pane, select the **Cloud App** tab.

The Cloud App tab lists information about the app provider, as well as a list of risk factors associated with the site.

For each risk factor described, an icon indicates whether it reduces risk (green circle) or increases risk (yellow triangle).



Because different risk factors carry different weights, a cloud app may be attributed medium or high risk, even when it has more risk-reducing factors than risk-increasing factors. This reflects the relative severity of the risk-increasing factors.

See *What risk factors does cloud app analysis look for?*, page 11, for a list of all of the risk factors that cloud app analysis considers.

What risk factors does cloud app analysis look for?

The risk factors considered when rating a cloud app include whether the app supports:

- File uploads
- Content posting
- Content sharing with users who do not have accounts within the application
- File or content sharing with a group of users (applies, for example, to storage services and social apps)
- Sharing data as a direct link
- The ability to immediately revoke access for internal or external users
- The ability for users to track their own usage history
- The ability for a third-party (like an employer) to track a user's usage history
- The ability for users to determine who accessed a particular object
- Two-factor authentication

- An applicative permission model (role-based permissions)
- Access restriction to specific endpoint devices, verified by certificate or other method
- The ability of users to save (remember) the app password on their endpoint device

Additional risk factors include:

- Who owns uploaded data
- What happens to a user's data in the app when the account is terminated
- The forms of authentication supported by the app provider
- Whether the app encrypts user data at rest
- Whether the company providing the app complies with the ISO 27001 standard
- Whether the company providing the app complies with the PCI DSS standard
- Whether the company providing the app complies with the HIPAA standard
- Whether the company providing the app complies with the SSAE-16 standard
- Whether the company providing the app complies with the SOC-1 standard
- Whether the company providing the app complies with the SOC-2 standard
- Whether the company providing the app complies with the ISAE-3402 standard