TRITON RiskVision Reporting Guide

Reporting Guide | TRITON RiskVision | Version 7.8

Use Websense TRITON RiskVision reporting tools to make sure your system is monitoring the expected traffic, and to investigate Internet activity.

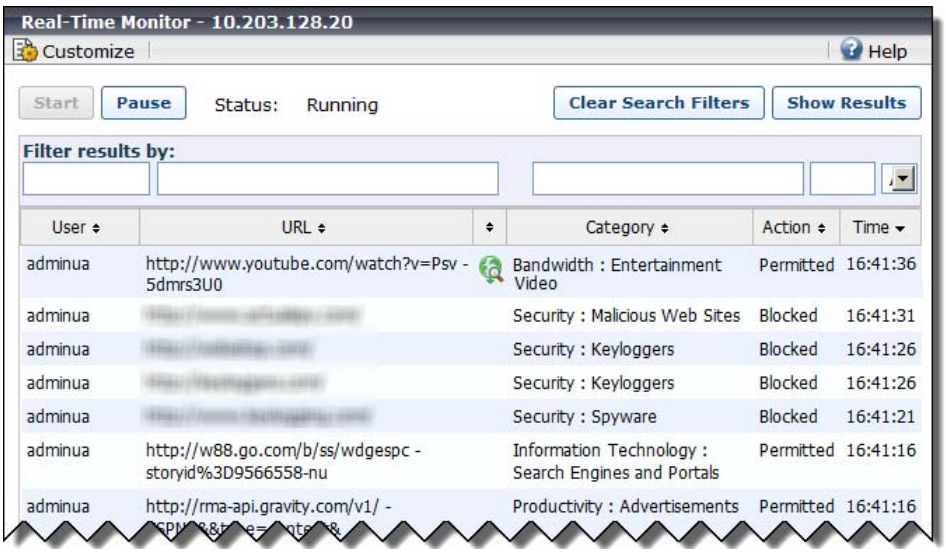
To get started, see:

Once you have verified that traffic is being monitored as expected, you can use a variety of reporting tools to understand and investigate threat activity and other Internet activity in your network.

See:

Validate your monitoring setup

Use Real-Time Monitor to get a snapshot of the traffic currently being monitored by your TRITON RiskVision deployment.



To start Real-Time Monitor:

1. Log on to the TRITON console and select the **RiskVision** module.
2. Navigate to the Reporting > **Real-Time Monitor** page.

If Internet traffic is visible to the SPAN port that your TRITON RiskVision appliance monitors, data begins to populate the page automatically, within a few seconds. If no data appears, make sure that:

- Your TRITON RiskVision appliance is connected to a SPAN port or a network tap that supports aggregation.
- Internet activity is being sent past the SPAN port or through the tap.
- The Content Gateway, Filtering Service, and Usage Monitor components are running on the appliance.
- Port 55835 is open from the appliance to the TRITON management server. Usage Monitor (on the appliance) uses this port to send data to Real-Time Monitor (on the management server).

Real-Time Monitor can show up to 1000 current Internet activity log records, displayed in a paged view with 25 results per page. Each record includes:

- The IP address or name of the **user** who made the request.
- The **URL** requested.
- Whether or not the requested site was recategorized as a result of Content Gateway analysis.

This is indicated by an icon to the right of the URL (as seen in the screenshot above).

- The **Category** assigned to the site.
- The **Action** flag (permitted or blocked) assigned to the request.
- The **Time** the request was passed to Real-Time Monitor.

To temporarily stop the flow of data, click **Pause** at the top of the screen. Click **Start** to resume updates.

You can sort the current data set by any of the columns on the page. For example, you can:

- Verify that traffic from a specific user or IP address is being seen.
- Focus on the requests that have been analyzed and recategorized by Content Gateway.

You can also use the filter fields at the top of the page to see only matching results. For example, look for traffic from a specific IP address or requests for a specific URL string. After entering a search string filter, click **Show Results**.

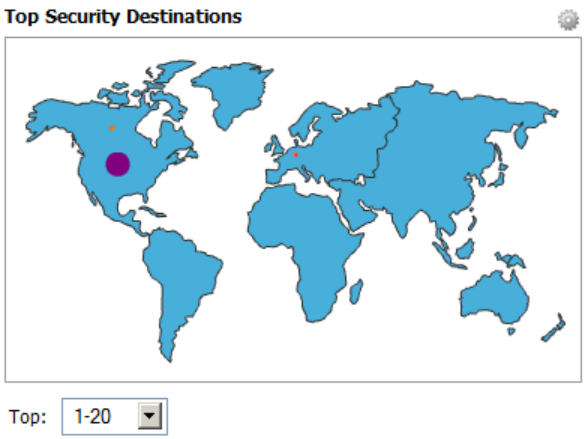
Click **Clear Search Filters** to review raw results.

Threat activity

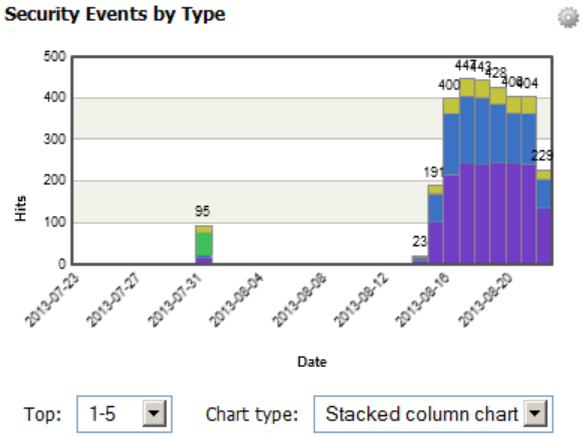
When you connect to the TRITON RiskVision manager, the Threats dashboard is displayed, giving an overview of suspicious activity that may be related to advanced malware threats in your network.

Use the charts near the top of the page to get a quick overview of recent threat-related activity:

- The **Top Security Destinations** map shows the top countries where suspicious traffic is being sent, or where sites associated with suspicious activity are hosted.



- The **Security Events by Type** chart shows the number of requests for sites (destinations) in the most frequently accessed security categories.



Click an item in the map or chart to filter the **Suspicious Event Summary** table at the bottom of the page. This shows only the incidents with the characteristic (destination country or category) you select.

The Suspicious Event Summary list is a starting point for more detailed investigation of threat activity.

Suspicious Event Summary Clear Customize Export To CSV

S	User	Device	Category	Last Attempt	CC	Incidents
C	[adminua]	10.203.128.20	Multiple	2013-08-14 13:17:00	US	2
H	10.201.67.45		Security: Keyloggers	2013-08-22 13:17:00	US	559
H	10.201.67.4		Security: Keyloggers	2013-08-22 13:17:00	Multiple	559
H	10.201.67.15		Security: Keyloggers	2013-08-22 13:09:00	DE	280
H	10.201.67.1		Security: Keyloggers	2013-08-22 13:09:00	US	280
H	[adminua]	10.203.128.20	Multiple	2013-08-14 16:41:00	Multiple	14
H	adminua	10.203.128.20	Security: Keyloggers	2013-07-31 13:28:00	Multiple	14
M	10.201.67.4		Security: Malicious Web Sites	2013-08-22 13:17:00	US	279
M	10.201.67.3		Security: Malicious Web Sites	2013-08-22 13:17:00	Multiple	432
M	Chekhov, Anton[achekhov]		Security: Malicious Web Sites	2013-08-22 13:04:00	US	280

By default, it includes the columns marked with an asterisk (*) below:

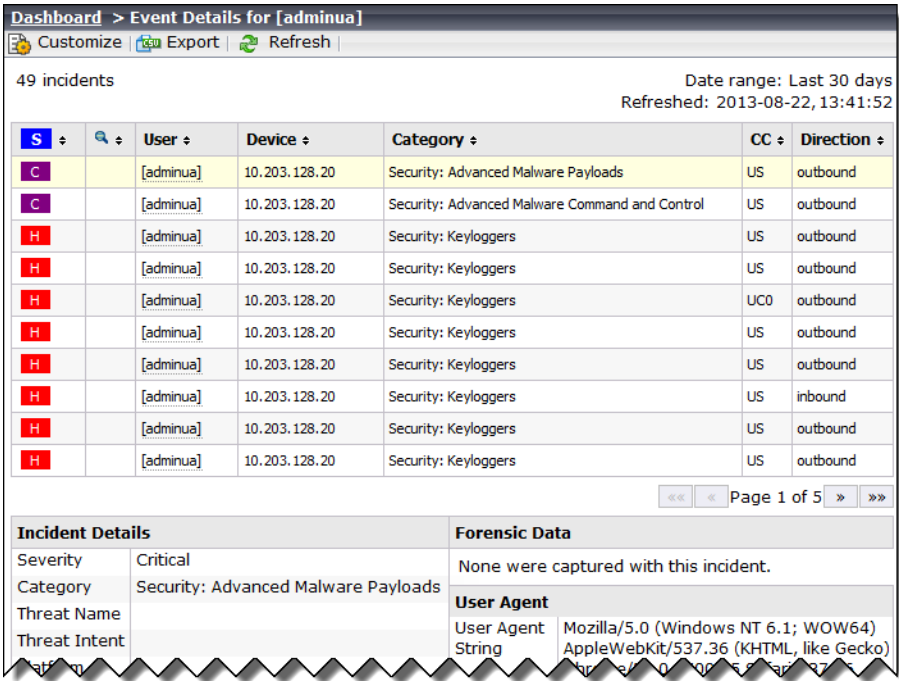
Column	Description
Severity*	Indicated by an “S” with a blue background (S). Shows the severity (Critical, High, Medium, or Low) assigned to the event.
Forensics*	Indicated by a magnifying glass ( ). Indicates whether the event included an attempt to send files.
User*	The user name (if any) associated with the activity.

Column	Description
IP address	The IP address of the machine on which the activity occurred.
Device*	The name of the machine on which the activity occurred, if available.
Category*	The Master Database category assigned to the activity.
Last Attempt*	The timestamp of the most recent event sharing all of the characteristics displayed in the row.
Country*	Indicated by the abbreviation “CC” (for country code). Shows the 2-letter country code for the event destination (target). If more than one destination is associated with an event, “Multiple” is displayed.
Direction	Whether the suspicious activity involved inbound or outbound traffic.
Incidents*	The number of incidents sharing the same user, IP address, and device of this severity level.

- Click **Customize** to change the columns shown.
- To investigate incidents for a user, IP address, or device, click the associated link in the summary list. This opens an **Event Details** page for the selected client.

The table at the top of the event details page shares a similar layout to the Suspicious Event Summary, but lists each incident individually.

Click a specific incident to show all of the data collected about that incident. This includes forensic data (if any) and the user agent header associated with the request.

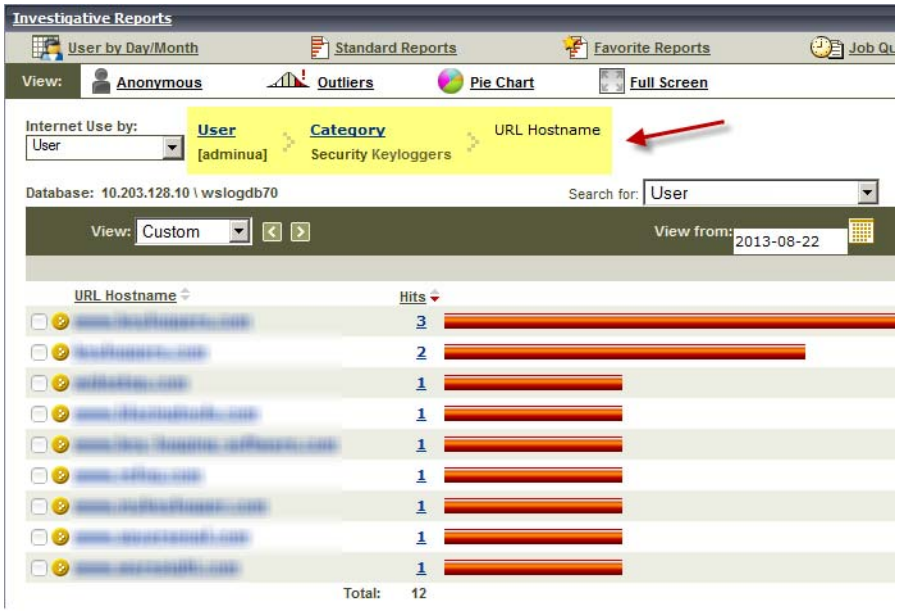


If forensic data was collected, use caution opening files that may be related to malicious activity. Note also that any file may contain sensitive data.

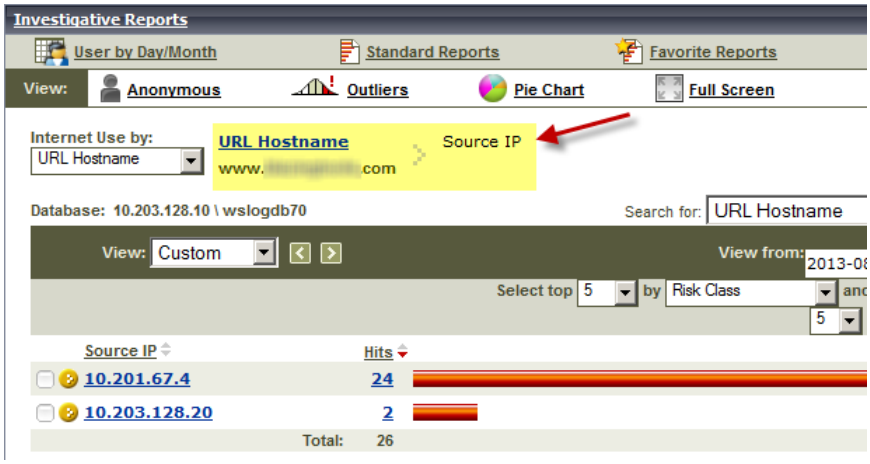
To gain a fuller picture of the threat presented by an incident, you can use the date, user, source IP address, and destination information (URL and IP address) to run investigative reports that give a more comprehensive picture of:

- Potentially related activity on the source machine

- Other suspicious activity associated with the user name



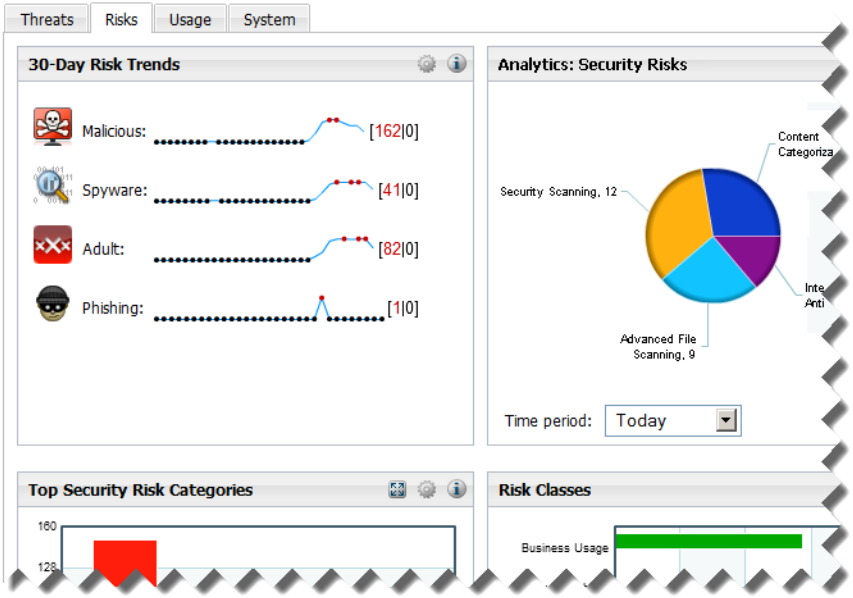
- Which other users or machines are requesting data from the suspicious destination (URL and IP address)



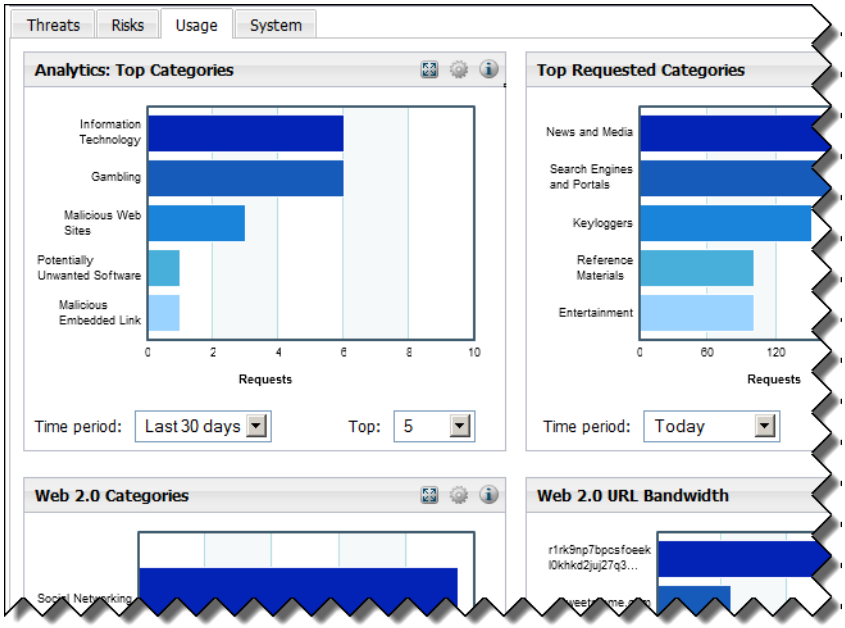
Monitor system activity

In addition to the Threats dashboard, the **Status > Dashboard** page includes dashboards that show:

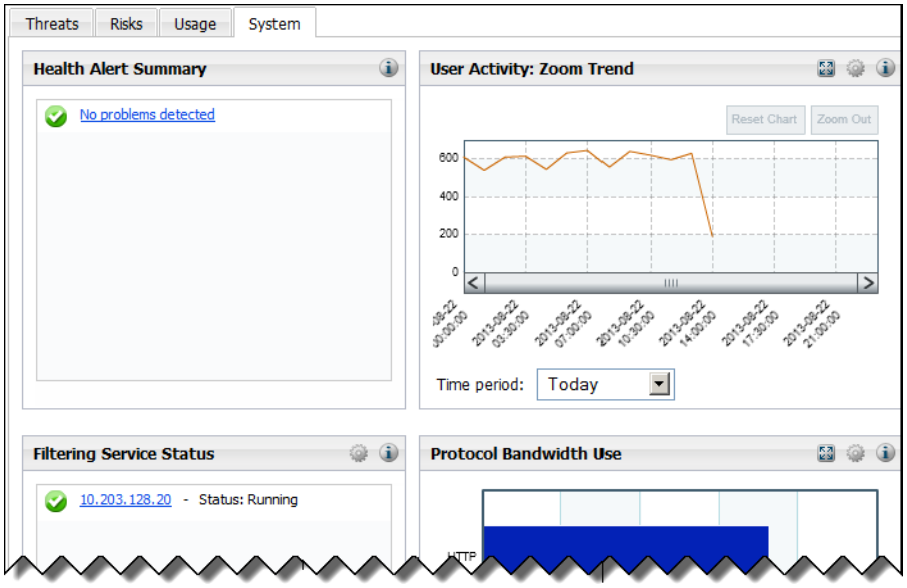
- **Risks** (including security risks, sorting of traffic into non-security risk classes, and uncategorized requests)



- **Usage** patterns (including top categories and summaries of analytic activity)



- **System** statistics (including a summary of active health alerts and a trend chart showing volume of monitoring activity)



Review the dashboard elements to get an overview of current system activity.

To delve more deeply, click a chart. This typically opens an investigative report that where you can manipulate the data to suit your needs. See *Dig deeper*, page 8, for more information.

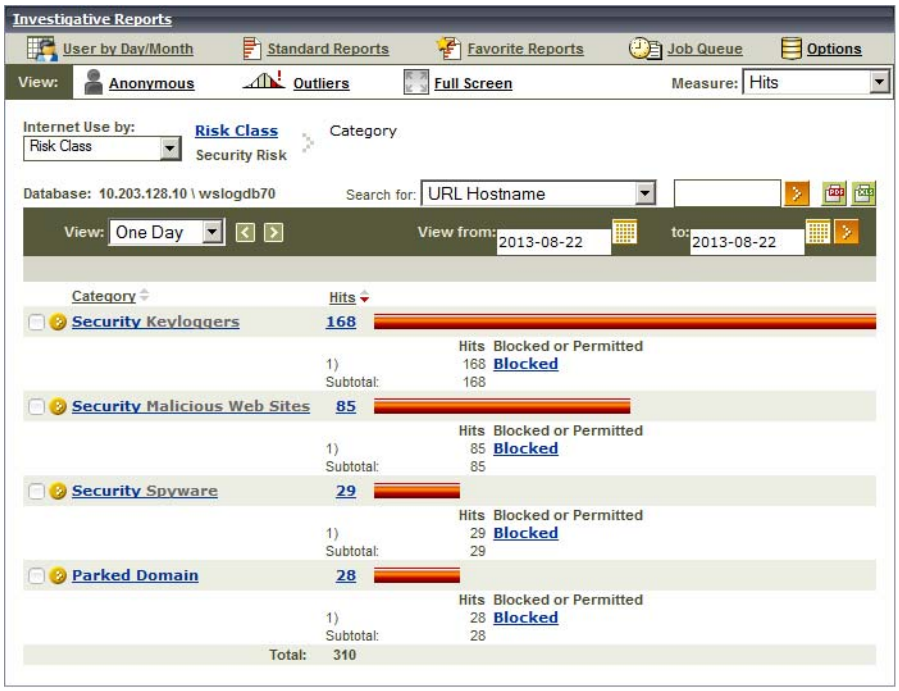
Dig deeper

Investigative reports are powerful and flexible. Dig as far as you need into the data you want to examine.

Launch an investigative report by clicking on a chart on the Risks, Usage, or System dashboard, or by navigating to the **Reporting > Investigative Reports** page in the TRITON RiskVision manager.

- If you click on a dashboard chart, the page shows the same data as the chart, but with many options for drilling into or expanding the data shown. For example:

- Clicking the **Top Security Risk Categories** chart opens a report showing the top security categories by hits, and whether the requests are flagged as permitted or blocked.



- Clicking the **Top Uncategorized** chart shows the top uncategorized URLs by hits.

- If you navigate directly to the page, a simple report is displayed that summarizes monitored and analyzed activity by **risk class**.

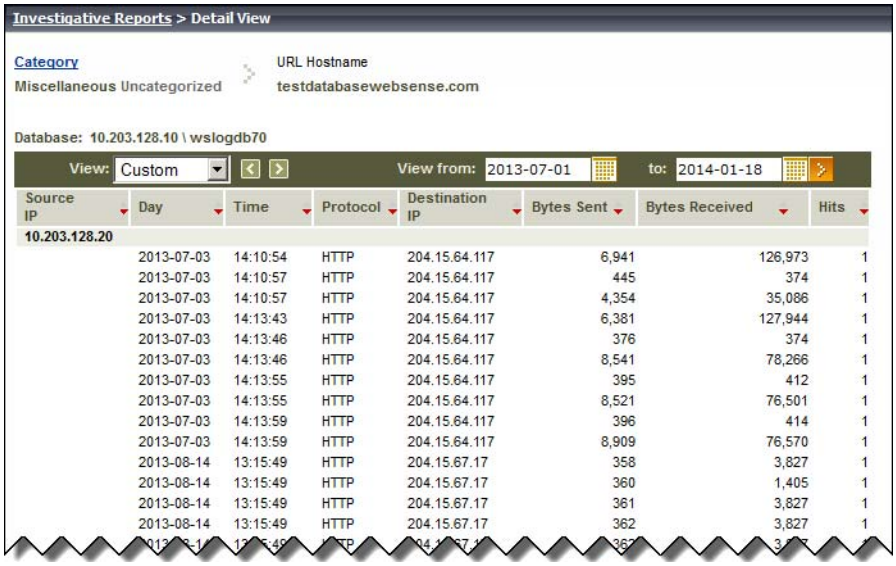
The risk classes are Security Risk, Legal Liability, Network Bandwidth Loss, Productivity Loss, and Business Usage.

From the initial report, you can:

- Click on the number of hits or volume of bandwidth (either the numeric value or the bar) to open a detail report.

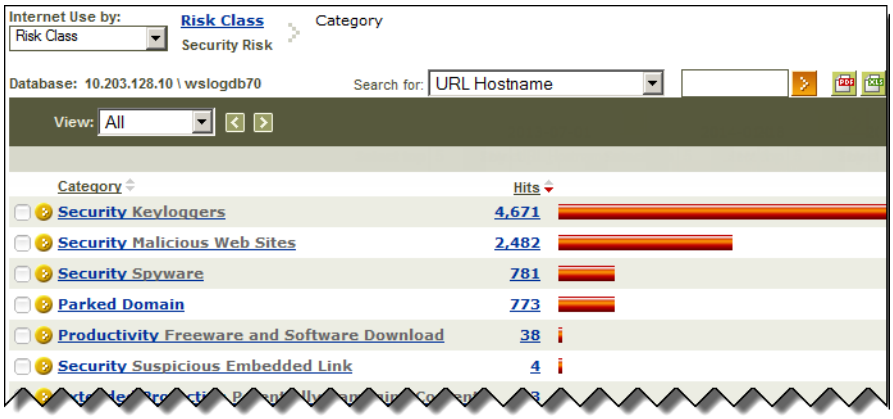
  For example, if you click on the number of hits for an uncategorized URL, the detail report shows the user requesting the site, the day the request was made, the action flag assigned to the request, and the protocol for each request (hit).

  To change which columns appear in the report, click **Modify Report**.



- Click an item in the leftmost column (risk class, category, user, URL, and so on) to see a list of options for drilling down into that type of data

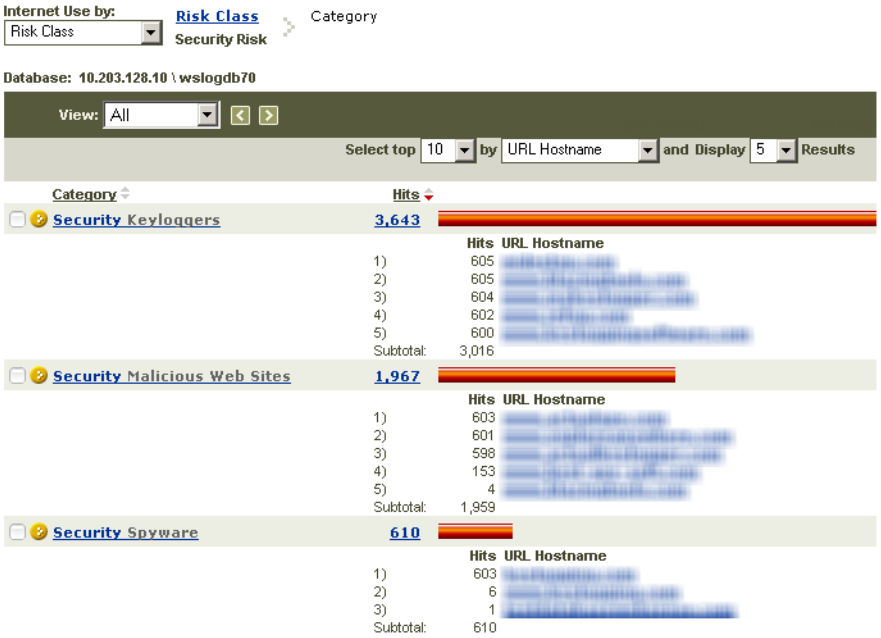
  For example, from the default summary report of all risk classes, expand the **Security Risk** entry and select **by Category**.



- Use the boxes in the gray toolbar above the report to further refine your results.

  For example, select top **10** by **URL Hostname** and display **5** results.

When you click **Display Results**, the report shows the 10 most requested Security Risk categories with the top 5 URL hostnames in each category.



You can also click **Standard Reports** in the toolbar at the top of the page to get a list of predefined reports. Click a report title to generate the report. The results can be modified just like any other investigative report.

For more details about using investigative reports to understand your data, see the TRITON RiskVision Investigative Reporting Quick Start (PDF).

Investigate data loss

Reporting Guide | TRITON RiskVision | Version 7.8

The Data Security manager offers several views into data loss detection activity, all accessed from the **Reporting > Data Loss Prevention** menu.

- Select **Dashboard** to get an overview of information leaks in the system and see what kind of violations have occurred in the last 7 days (default).

  The dashboard provides a balanced view and a high-level summary of incidents to give you an overall picture of information leaks in the network.

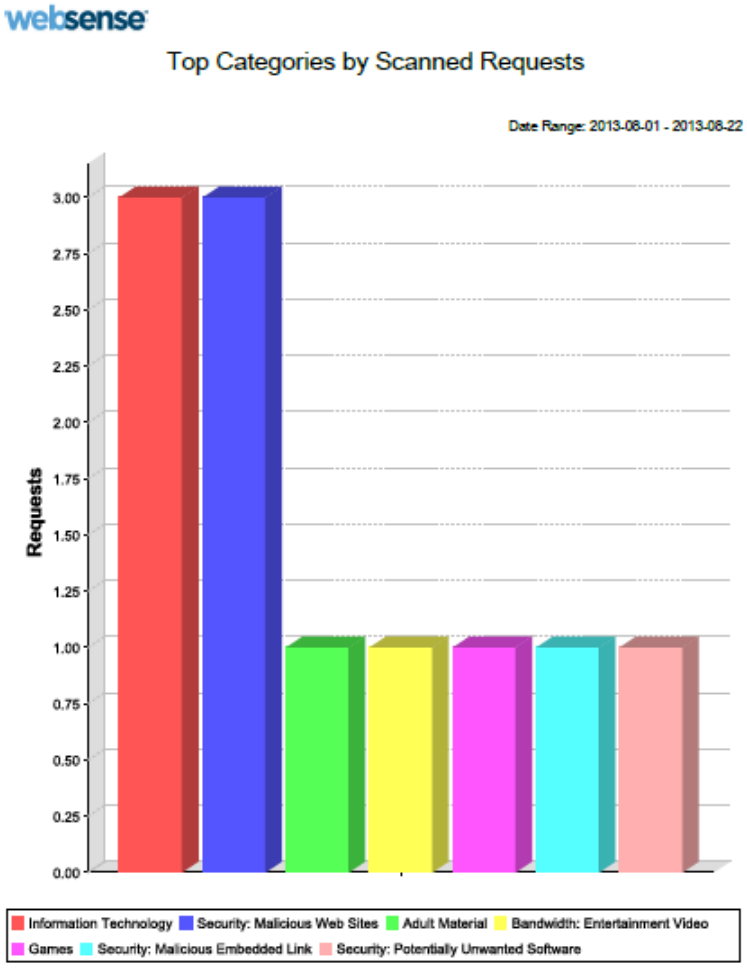
- Select **Incidents** (last 3 days or last 7 days) to see detailed information about each detected data loss incident, and to manage incident workflow, remediation, and escalation.

  The incidents list is a table displaying all data loss detection incidents, sorted by incident time (default). The table can be sorted by any column, and you can customize the types of details shown.

  Select an incident to view details about it in the bottom portion of the screen.

Share results with others

Use presentation reports to create bar charts, trend charts, or tabular reports showing Internet monitoring and analysis activity in HTML, PDF, or Microsoft Excel (XLS) format.



Administrators may want to generate presentation reports:

- For those who prefer a report they can print and review, rather than an online, drill down report.

  Presentation reports may be more readable or usable to some consumers than investigative reports.

- After drilling down into investigative reports data requiring additional analysis.

  Some presentation reports provide more detailed information for comparisons over a longer time period, across more users, or including more categories.

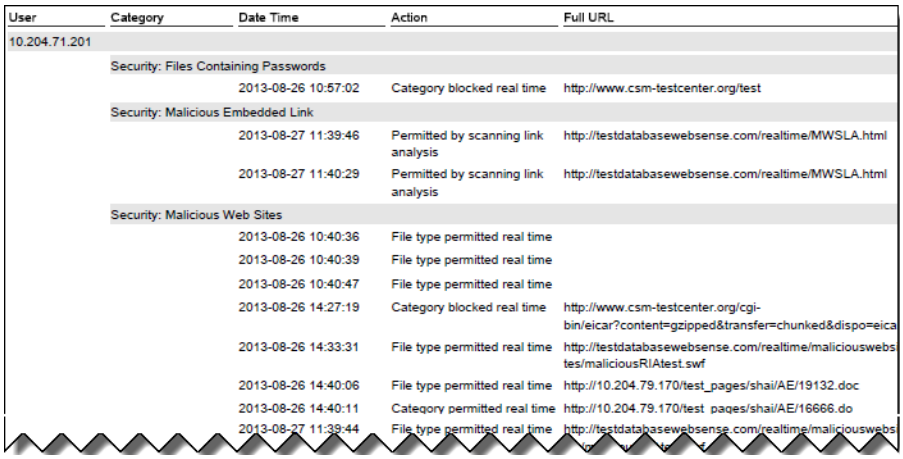
Run presentation reports on the **Reporting > Presentation Reports** page in the TRITON RiskVision manager. The page initially displays a Report Catalog that lists the available predefined and custom reports.

- Expand a report category in the catalog to see the reports it contains.
- Select a report in the tree to **Run** it, **Edit** it (custom reports only), or create a copy (via the **Save As** option).
  - Although predefined reports cannot be edited, you can create a copy of the report and use that as a basis for generating a custom version of the report.
  - Copies of predefined and custom reports can be edited without affecting the report that they're based on.

When you select a template (in the catalog under **Base Templates**), the Run option is not available. Click **Save As** to start the process of creating a custom report.

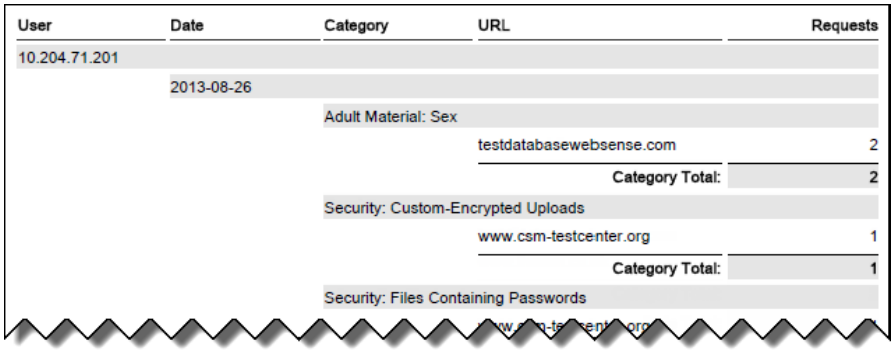
Useful reports for learning more about the results of Content Gateway analysis can be found in the Scanning Activity section of the report catalog. For example:

- If you have enabled full URL logging, the **Scanned: Detail of Full URL** report shows the results of URL, broken down by user and category.



User	Category	Date Time	Action	Full URL
10.204.71.201				
	Security: Files Containing Passwords			
		2013-08-26 10:57:02	Category blocked real time	http://www.csm-testcenter.org/test
	Security: Malicious Embedded Link			
		2013-08-27 11:39:46	Permitted by scanning link analysis	http://testdatabasewebsense.com/realtime/MWSLA.html
		2013-08-27 11:40:29	Permitted by scanning link analysis	http://testdatabasewebsense.com/realtime/MWSLA.html
	Security: Malicious Web Sites			
		2013-08-26 10:40:36	File type permitted real time	
		2013-08-26 10:40:39	File type permitted real time	
		2013-08-26 10:40:47	File type permitted real time	
		2013-08-26 14:27:19	Category blocked real time	http://www.csm-testcenter.org/cgi-bin/eicar?content=gzipped&transfer=chunked&dispo=eica
		2013-08-26 14:33:31	File type permitted real time	http://testdatabasewebsense.com/realtime/maliciouswebs tes/maliciousRIAtest.swf
		2013-08-26 14:40:06	File type permitted real time	http://10.204.79.170/test_pages/shai/AE/19132.doc
		2013-08-26 14:40:11	Category permitted real time	http://10.204.79.170/test_pages/shai/AE/16666.do
		2013-08-27 11:39:44	File type permitted real time	http://testdatabasewebsense.com/realtime/maliciouswebs

- **Summary of Scanned Requests by User** gives a breakdown of the results of analysis for users (or, if user name information is not available, source IP addresses) in your network.



User	Date	Category	URL	Requests
10.204.71.201				
	2013-08-26			
		Adult Material: Sex		
			testdatabasewebsense.com	2
			Category Total:	**2**
		Security: Custom-Encrypted Uploads		
			www.csm-testcenter.org	1
			Category Total:	**1**
		Security: Files Containing Passwords		

If you are not using policies that apply the block flag to requests, the following pre-defined presentation reports do not apply:

Security Threats

- Security Risk Sites Blocked by Date
- Users Blocked from Security Risk Sites by Date

Policy Enforcement

- Top Blocked Categories by Requests
- Top Blocked Groups by Requests
- Top Blocked Protocols by Requests
- Top Blocked Sites by Requests
- Top Blocked Users by Requests
- Top Filtering Actions by Requests

Real Time Security Threats

- Blocked Files by Security Threat
- Blocked Security Risk Files by User
- Blocked Security Risk Sites by Requests
- Blocked Security Risk Sites by User
- Detail of Blocked Security Risk Files by User
- Detail of Blocked Security Risk Sites by User
- Detail of Blocked Security Threats by User
- Stripped Content Types by User
- Top Blocked Files by Security Threats
- Top Blocked Security Risk Sites by Requests
- Top Blocked Security Threats by Requests
- Top Blocked Users by Security Risk Files
- Top Users Blocked from Security Risk Sites

Scanning Activity

- Top Sites Blocked by Link Analysis

Click **Help > Explain This Page** from the Presentation Reports page to find detailed information about running, customizing, and using presentation reports.