

v2.0.0 Release Notes for TRITON RiskVision

52080 | Release Notes | TRITON RiskVision | 24-Sep-2015

This release introduces TRITON® RiskVision™ 2.0: the next generation of TRITON threat monitoring and risk analysis.

RiskVision 2.0 resides on a V10000 G4 appliance. When connected to a port mirror, it analyzes HTTP and SMTP traffic to detect malware, data loss, and data theft activity, as well as suspicious or potentially risky transactions. When used in conjunction with an SSL decryption product, RiskVision can also analyze HTTPS traffic.

In this release, the RiskVision appliance can use a single interface for monitoring and capturing traffic.

For more information about this release, see:

- ◆ [RiskVision v2.0.0 Features, page 2](#)
- ◆ [Known issues for RiskVision v2.0.0, page 7](#)

For deployment and installation information, see:

- ◆ [Quick Start Poster for the Websense V10000 G4 TRITON RiskVision Appliance](#) (PDF): contains information for racking, cabling, and powering on the appliance, as well as an overview of the installation process.
- ◆ [TRITON RiskVision Setup Guide](#) (PDF): contains detailed installation and initial configuration instructions.

RiskVision v2.0.0 Features

52081 | Release Notes | TRITON RiskVision | 24-Sep-2015

TRITON RiskVision offers administrators:

- ◆ A simple, one-appliance deployment
- ◆ Fast and easy setup
- ◆ A flexible, plugin-based architecture for extensibility and interoperability
- ◆ Detailed insight into malicious software activity in HTTP and SMTP traffic
- ◆ Data loss and data theft detection

Read on for more detailed information about the features and tools offered in this release.

Interactive incident investigation

The RiskVision Transaction Viewer is an interactive tool that administrators can use to find and investigate high-priority incidents in their network. The tool offers:

- ◆ Filtering, grouping, and sorting capabilities to help administrators to identify the incidents with most potential to cause harm
- ◆ A comprehensive details pane to help administrators assess the threat

The screenshot displays the RiskVision Transaction Viewer interface. At the top, there is a search filter and a 'View details' button. Below this, a table lists incidents with columns for Session, Threat Level, Client IP, Threat Name, Incident Time, and Data Content. The table is filtered to show incidents from the 'CryptoWall' threat, specifically those from the client IP 192.168.138.158. The incidents listed have a 'Malicious' threat level and are categorized as 'Suspected malware communication'. Below the table, a 'Transaction Details' pane is open, showing information for a specific transaction. The details are organized into 'General' and 'Advanced' sections. The 'General' section includes fields for Analytic-Assigned Category, Method, Destination IP, Data Content, Severity, File Size, File Name, Transactional Processing Flags, Plugins, and Reason. The 'Advanced' section includes Client IP, URL Category Names, Destination Port, Content Classifier, SHA-1 Hash, File Type, HTTP Return Code, and PCAP Location.

Session	Threat Level	Client IP	Threat Name	Incident Time	Data Content
313	Malicious	192.168.138.158	CryptoWall	2015-05-07 13...	Suspected malware communication
312	Malicious	192.168.138.158	CryptoWall	2015-05-07 13...	Suspected malware communication
311	Malicious	192.168.138.158	CryptoWall	2015-05-07 13...	Suspected malware communication
310	Malicious	192.168.138.158	CryptoWall	2015-05-07 13...	Suspected malware communication
309	Malicious	192.168.138.158	CryptoWall	2015-05-07 13...	Suspected malware communication
308	Malicious	192.168.138.158	CryptoWall	2015-05-07 13...	Suspected malware communication

Transaction Details

General

Analytic-Assigned Category: Bot Networks
Method: POST
Destination IP: 72.34.49.86
Data Content: Suspected malware communication
Severity: High
File Size: 162 B
File Name: img5.php
Transactional Processing Flags: LogIssue, RunAnalytics
Plugins: Content Analysis, Data Analysis, URL Lookup
Reason: 0-23591-CryptoWall.Backchannel_Traffic.Web.RTSS

Advanced

Client IP: 192.168.138.158
URL Category Names: Bot Networks
Destination Port: 80
Content Classifier: Suspected malware communication
SHA-1 Hash: 51fe7f6216c59204b24...
File Type: Text
HTTP Return Code: 200
PCAP Location: /opt/websense/data/pcaps/preserved/0000000311_001_1431031908...

The Transaction Viewer combines the information returned by both local and cloud-based analysis tools, giving administrators detailed insight into why a malicious or suspicious incident was identified within a transaction.

Comprehensive local analysis

When RiskVision processes a transaction, it uses several analytic tools on the appliance to determine whether the transaction contains any malicious or suspicious characteristics. Together, these analytics are grouped together under the term Local Analysis.

- ◆ **URL lookup** is used to determine whether HTTP requests are going to sites already known to pose a security risk
- ◆ **Content analysis** uses Websense Advanced Classification Engine (ACE) technologies to find malicious and suspicious behavior within an HTTP or SMTP transaction
- ◆ **Data analysis** uses data loss and data theft policies to detect sensitive data leaving the network via HTTP or SMTP transactions
- ◆ **Cloud app analysis** is used to identify traffic to cloud applications that may present malware, compliance, or data loss risks to the organization
- ◆ **YARA analysis** is provided for organizations that already use YARA for malware classification. When enabled, the RiskVision YARA Plugin tries to match YARA rules within each transaction to find evidence of malware.

RiskVision also offers the ability to send incident information to a third-party SIEM tool or syslog for further investigation.

Cloud-based file sandboxing

When RiskVision Local Analysis does not find malicious characteristics in its file analysis, it may recommend that the files go through further investigation from the Websense File Sandbox.

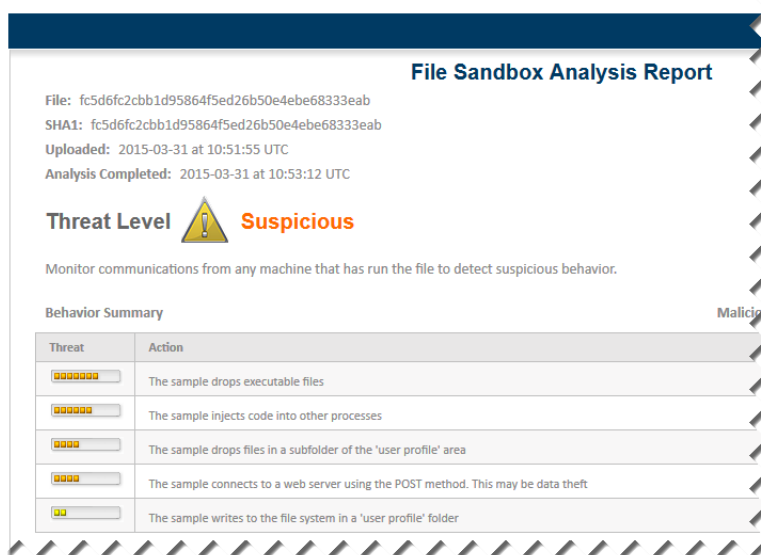
When a file is flagged for sandboxing, the File Sandbox Processor contacts the File Sandboxing service in the cloud to find out if the file has been analyzed previously.

- ◆ If so, File Sandbox Processor requests the analysis results.
- ◆ If not, the file is uploaded to the sandbox environment, where it can be run and examined to determine whether its behavior is consistent with malicious activity.

File Sandbox Processor polls occasionally for results.


When File Sandboxing has completed its analysis, it creates an online report that details its findings. File Sandbox Processor retrieves a link to the report, and adds it to the RiskVision incident record.

Websense® File Sandboxing








File Sandbox Analysis Report

File: fc5d6fc2cbb1d95864f5ed26b50e4ebe68333eab
SHA1: fc5d6fc2cbb1d95864f5ed26b50e4ebe68333eab
Uploaded: 2015-03-31 at 10:51:55 UTC
Analysis Completed: 2015-03-31 at 10:53:12 UTC

Threat Level  **Suspicious**

Monitor communications from any machine that has run the file to detect suspicious behavior.

Behavior Summary Malicious

Threat	Action
	The sample drops executable files
	The sample injects code into other processes
	The sample drops files in a subfolder of the 'user profile' area
	The sample connects to a web server using the POST method. This may be data theft
	The sample writes to the file system in a 'user profile' folder

RiskVision administrators can access the link from the Transaction Viewer.

Comprehensive risk reporting

RiskVision includes several pre-defined malicious activity and data analysis reports that can be generated either individually, or as part of a comprehensive incident assessment. These reports are available in PDF or RTF format, and include a combination of summary and detail reports in tabular and chart formats.



Incident Assessment

Top Cloud Apps by Risk Level (from 07-31-2014 at 00:00 to 07-01-2015 at 00:00)

Many factors contribute to the risk level assigned to a cloud app, from the practices of the company that provides the app and security technology within the app to the ways that end users can use the app. Combine the general cloud app assessment from RiskVision with data loss data, your organization's own guidelines about cloud app usage, and information about your users to determine a response to the information in these reports.

High risk apps: **10**

Top 5 App Summary

Cloud App	Risk Level	Users	Bandwidth
HR-Meter	High	199	3.85 MB
Talisma Fundraising	High	145	7.21 MB
Dremus	High	28	22.43 KB
Freightquote	High	635	39.04 MB
Ofipro	High	57	1.02 MB

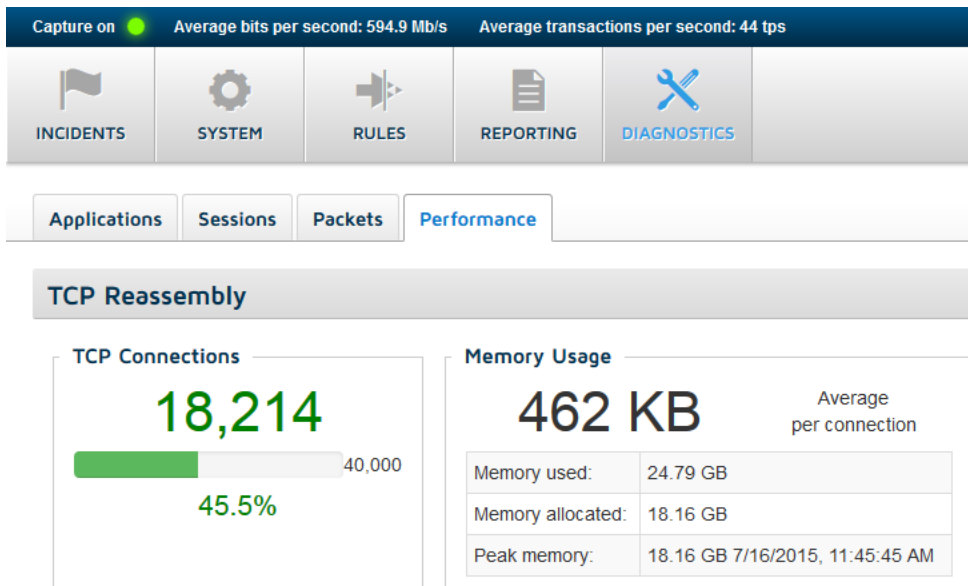
Risky Cloud Apps

Cloud App	URL	Risk Level	Users	Bandwidth	Last Seen
HR-Meter	http://www.hr-meter.com	High	199	3.85 MB	04-20-2015
HR-Meter is an international full service Human Resources consultancy firm that offers our world class clients across the globe innovative assessment services with a unique and unprecedented level of customization.					
Talisma Fundraising	http://www.campusmanagement.com	High	145	7.21 MB	04-23-2015
Campus Management Corp.'s mission is to deliver superior technology solutions that enable institutional excellence for higher education institutions and philanthropic non-profit organizations.					
Dremus	http://www.dremus.com	High	28	22.43 KB	04-23-2015
Dremus is an online selling tool for business, a totally customizable hosted e-commerce solution.					
Freightquote	http://www.freightquote.com	High	635	39.04 MB	05-07-2015
Freightquote delivers a vast array of freight services for a large and diverse customer base. These services enable customers to instantly quote and compare the shipping rates of hundreds of national and regional freight carriers.					
Ofipro	http://www.ofipro.es	High	57	1.02 MB	04-20-2015
Ofipro is a Online Business Solution for Freelancers, Small and Medium Business and Accountants.					

User-friendly diagnostic tools

The **Diagnostics** page in the RiskVision Local Manager offers tools and statistics to help administrators:

- ◆ Verify that the system is running correctly
- ◆ Monitor system performance
- ◆ Identify issues quickly
- ◆ Pinpoint the component or function that is experiencing a problem



In addition, the Local Manager offers interfaces for administrators to start or restart services, verify database downloads, and configure network interface use.

Known issues for RiskVision v2.0.0

52082 | Release Notes | TRITON RiskVision | 24-Sep-2015

As a best practice, TRITON RiskVision administrators are encouraged to update their deployment as soon as possible after setting up the system. Use the **System > Updates** tab of the Local Manager to keep the operating system and RiskVision software current with the latest hotfixes, patches, and upgrades.

As fixes are found for these known issues, the Updates tab will display a notification that system updates are available.

Transaction Viewer

- ◆ In the Transaction Viewer, a threat level of **No threat detected** indicates that no local or cloud analytics found characteristics indicating malicious, suspicious, or data loss activity.

This is true in either of the following cases:

- All analytics successfully analyzed the transaction and found no threat.
- No analytic returned a threat score due to errors or timeouts.

The Transaction Viewer does not currently indicate whether a threat level of “no threat detected” is based on completed or failed analysis.

This issue is being tracked as TRV-1893 and 1894.

- ◆ The Excel button above the Transaction Viewer is intended to generate a CSV file containing all incident records in the database. Currently, clicking the button has no effect. No file is generated.

This issue is being tracked as TRV-1918.

Analysis

- ◆ In rare cases, the Data Analysis Plugin does not return results before the RiskVision timeout period ends. When this occurs, the Transaction Viewer simply does not show any Data Analysis results for a transaction.

If you encounter this problem, it will be reflected in the **Data Analysis Plugin > Total failed analysis** statistic on the Local Manager **Diagnostics > Performance** page.

This issue is being tracked as TRV-1683.

- ◆ In some cases, the File Sandbox Processor plugin incorrectly reports that File Sandboxing is not available. When this occurs:

- Files are not submitted for sandboxing.
- File Sandbox Processor does not poll for sandboxing results.

If this problem occurs, administrators can resolve it by restarting the **File Sandbox Processor** service on the **System > Services** page in the Local Manager.
This issue is being tracked as TRV-1912.

Rules

- ◆ On the Rules page, the description of the default internal network rules are incorrect. Internal network rules are used to distinguish between internal and external traffic in order to determine traffic direction (inbound or outbound), and do not have anything to do with whitelisting.

This issue is being tracked as TRV-1915.