v2.1.0 Release Notes for TRITON RiskVision

Release Notes | TRITON RiskVision | 06-Jun-2016

TRITON® RiskVision™ 2.1 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.

The RiskVision appliance can use a single interface for monitoring and capturing traffic.

For more information about this release, see:

- *New in RiskVision v2.1.0*, page 2
- *Upgrading to RiskVision 2.1*, page 7
- *Resolved and known issues for RiskVision v2.1.0*, page 8

For deployment and installation details for new RiskVision deployments, see:

- Quick Start Poster for the 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.

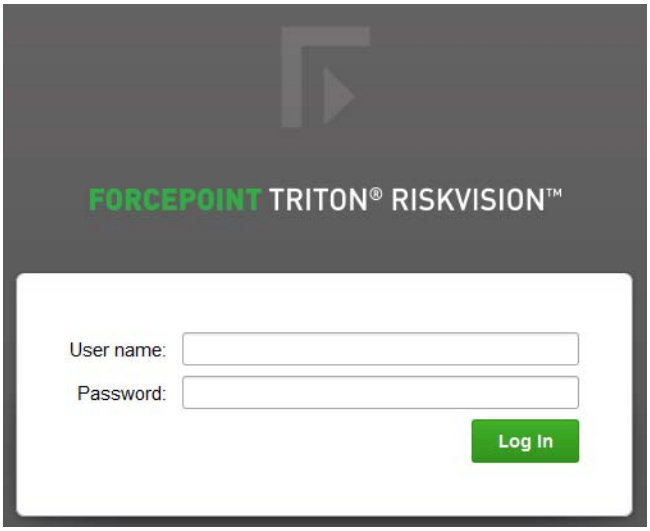
© 2016 Forcepoint LLC

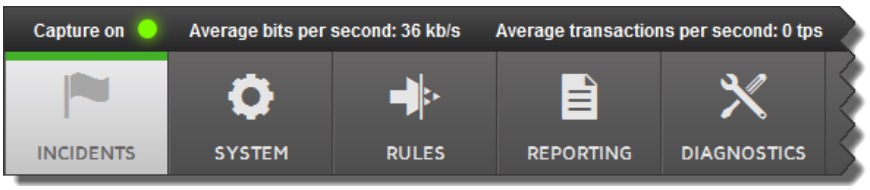
New in RiskVision v2.1.0

Release Notes | TRITON RiskVision | 06-Jun-2016

Look and feel enhancements

To support the transition from Raytheon | Websense to Forcepoint LLC, the RiskVision Local Manager has a new look and feel. The colors and logos throughout the management console, including the logon screen and toolbar, have been updated to reflect the Forcepoint brand.





Similar changes have been made in the Help system, as well as in external content, like the Knowledge Base and Support portal.

As a result of the creation of Forcepoint LLC, the RiskVision subscription agreement has been updated for v2.1. If you are upgrading from v2.0, be sure to accept the new subscription agreement after upgrade is complete. See *Upgrading to RiskVision 2.1*,

page 7, for complete upgrade instructions.

Important

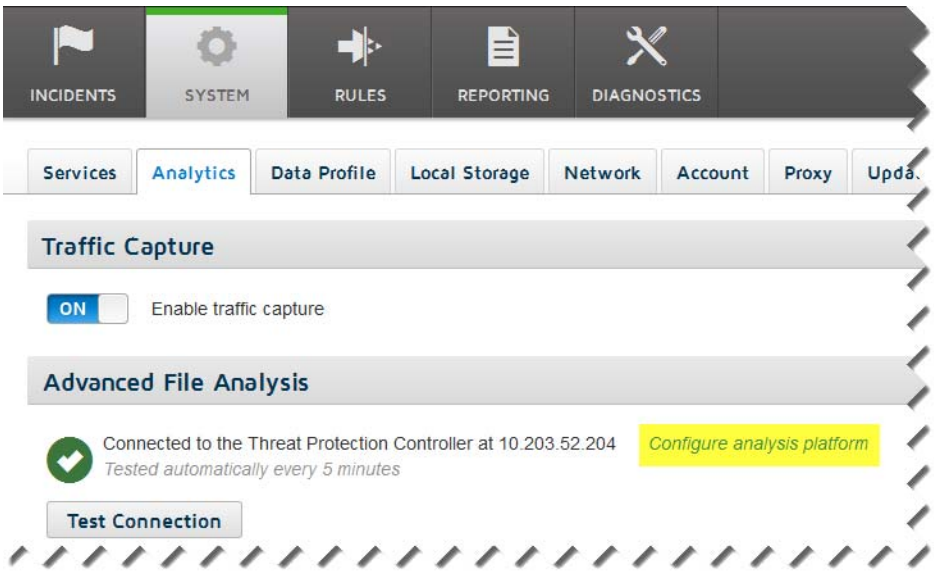
If you are upgrading from version 2.0, and are using a custom SIEM or syslog format, the vendor will continue to be reported as Websense until you manually update the format string.

If you are using a pre-defined SIEM or syslog format, the vendor will be updated to Forcepoint automatically.

Integration with Threat Protection Appliance

RiskVision customers who also have SureView Threat Protection Appliance now have the option to forward suspicious files to either the cloud-based File Sandbox or to the Threat Protection Appliance for additional analysis.

Configure which file analysis tool to use on the **System** > **Analytics** page in the RiskVision Local Manager.



To configure RiskVision to forward files to Threat Protection Appliance:

1. Click the **Configure analysis platform** link on the System > Analytics page.
2. Select the **Threat Protection Appliance** radio button.
3. Enter the **IP address** for the **prod1** interface of the Threat Protection Controller.
4. Click **OK**.

In incident records, if file analysis occurred, the **Plugins** field specifies whether the File Sandbox or Threat Protection Appliance performed the analysis.

Enhanced support for YARA rules

In this version, in addition to supporting customer-supplied YARA rules, RiskVision automatically downloads a YARA rules database, similar to its other analytic databases.

In this release, the YARA rules are used only to identify macros in text files. Files containing macros are flagged for further processing by Threat Protection Appliance.

RiskVision downloads YARA rules from Forcepoint download servers and saves them in the **/opt/websense/yara/download** directory on the appliance.

- RiskVision checks for updates daily.
- Downloaded YARA rules are encrypted, and cannot be edited directly by RiskVision administrators.
- Administrators can prompt RiskVision to reload all of its YARA rules by creating an empty file called **update** in the **/opt/websense/yara/** directory.
  - The update occurs within 5 minutes, and does not require restarting any services.
  - When the update is complete, the YARA plugin deletes the empty “update” file.

The Yara Plugin section of the Diagnostics > Performance page has been expanded to include information about decryption of the YARA database.

Yara Plugin

Compiled rule files:	3
Decrypted rule files:	1
Files detected:	4
Matched rules:	7
Rules found bad:	0
Scans failed:	0
Scans timed out:	0

Note

In addition to using rules from the Forcepoint YARA database, you can also configure RiskVision to apply your own custom YARA rules. See the Using YARA Rules with RiskVision technical paper for details.

Enhanced incident details

When you select an incident in the Transaction Viewer, the Detail pane now includes:

- A link to the VirusTotal website

  The link includes the SHA-256 hash for the file associated with the incident. If a VirusTotal report exists for the file, clicking the link opens the report in a new browser tab.
- The SHA-256 hash for the file associated with the incident

  This supplements the SHA-1 hash that is also displayed.
- A list of Transactional Processing Flags (if any) that local analytics have appended to the incident

  The flags that may be set by RiskVision analytics include:

  - **Detected by Yara** indicates that the incident was matched to a YARA rule by the YARA Plugin.
  - **OffBoxScanRequired** indicates that Local Analysis determined that a file should be further analyzed by the File Sandbox.
  - **OffBoxTPScanRequired** indicates that Local Analysis determined that a file should be further analyzed by the Threat Protection Appliance.
  - **Persist** indicates that the incident needs to be logged to the database.
  - **RunAnalytics** indicates that the User/URL Lookup plugin determined the Content Analytics Plugin should perform analysis.

  In addition, any labels added to an incident by custom YARA rules are displayed here.

Updates to SIEM and syslog logging

A new field, **sourceServerIp**, has been added to the default SIEM/syslog formats. This reports the IP address of the RiskVision appliance that analyzed an incident.

In addition, several other SIEM keys may now optionally be included in custom SIEM and syslog strings:

Key Name	Description
bytesReceived	Number of bytes received by the source machine
bytesSent	Number of bytes sent from the source machine
cloudName	Name of the cloud app associated with the incident
cloudRiskLevel	Risk level associated with the cloud app accessed as part of the incident
dbCategories	List of category codes returned by the analytic plugins
fileHash256	SHA-256 hash of the analyzed file

Key Name	Description
filnameOnDisk	Full path to the analyzed file on the RiskVision appliance
httpReturnCode	HTTP status code returned in response to a request
nCategories	Total number of categories assigned to an incident by the analytic plugins
pcapLocation	Full path to a PCAP file on the RiskVision appliance
platform	Indicates the advanced file analysis platform: File Sandbox or Threat Protection
pluginType	Internal name of each analytic plugin that returned results for the incident
reportURL	A link to the File Sandboxing or Threat Protection Appliance report (if any) associated with an incident
threatStage	Stage of the advanced malware threat kill chain the analyzed file represents
txnDate	Date the transaction occurred, in ISO format

Upgrading to RiskVision 2.1

To upgrade a RiskVision 2.0 appliance to version 2.1:

1. Log in to the **RiskVision Local Manager**.
2. Navigate to the **System > Updates** page.
3. Click **Start Update**.
4. When prompted, click **OK**.

   The upgrade will take a few minutes to complete. During the upgrade process, you will be logged out of the Local Manager and the appliance will reboot.
5. After the upgrade process has completed, log in to the RiskVision Local Manager.
6. Navigate to the **System > Account** page.
7. Review and accept the updated Forcepoint **Subscription Agreement**.

   You must accept the subscription agreement in order for RiskVision to resume traffic analysis.

If you need to reinstall RiskVision 2.1 from scratch, a recovery image is available from the **Downloads** tab of the **My Account** page at **forcepoint.com**. See Reinstalling RiskVision from a USB Drive for detailed instructions.

Resolved and known issues for RiskVision v2.1.0

Release Notes | TRITON RiskVision | 06-Jun-2016

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.

Resolved Issues

General

- If RiskVision is unable to submit a file for file sandboxing due to repeated errors or timeouts, the File Sandboxing result in the Transaction Viewer is updated to indicate that an error occurred. (TRV-1893)
- The Transaction Viewer option to export incident records to a CSV file works correctly. (TRV-1918)
- The File Sandbox Processor successfully recovers without administrator intervention when File Sandboxing is temporarily unavailable. (TRV-1912)
- The description of internal network rules on the Rules page has been corrected. (TRV-1915)
- When the RiskVision subscription expires, an alert badge is now displayed on the System tab of the Local Manager toolbar. (TRV-2039)

Vulnerability fixes

- A vulnerability that could have allowed a cross-site request forgery (CSRF) attack in the Local Manager has been addressed by introducing the use of a random token (X-XSRF-TOKEN). (TRV-2054)
- Local Manager session timeout behavior has been improved to ensure that administrators are logged out after 10 minutes of inactivity. (TRV-2055)
- Information that could expose Local Manager services to attack has been removed from error messages. (TRV-2057)

Known Issues

- If you enter a subscription key in the RiskVision Local Manager before accepting the Forcepoint Subscription Agreement, an error message is displayed, stating that the key is invalid.

To work around this issue, accept the Subscription Agreement first, then enter the subscription key. (TRV-2070)

- 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. (TRV-1683)