v7.8.1 Release Notes for Websense® TRITON® RiskVision™

Topic 50630 | Release Notes | TRITON RiskVision | v7.8.1 | 22-Oct-2013

Use the Release Notes to find information about TRITON RiskVision features, installation, and operation.

Introducing TRITON RiskVision

Topic 50631 | Release Notes | TRITON RiskVision | v7.8.1 | 22-Oct-2013

Websense TRITON RiskVision monitors Internet traffic by connecting to the SPAN or mirror port on a switch, or to a network tap that supports aggregation. That monitored traffic is then analyzed by the following TRITON RiskVision components and features to identify threat-related activity:

- Websense Advanced Classification Engine (ACE) analytics analyze requests and responses in real time. Administrators can:
  - Use dashboard charts, reporting tools, and Real-Time Monitor to investigate and understand the results of this analysis.
  - Enable suspicious activity and usage alerts to be notified about types of detected Internet activity of interest to the organization.
- ThreatScope Cloud Services provide sandboxing to find advanced malware threats in suspicious files. Administrators can:
  - Receive ThreatScope alerts when file analysis is complete.
  - Access online ThreatScope reports to learn more about analyzed files, the threats associated with them, and steps needed for remediation.
  - Use investigative reports to find more information about Internet activity on machines where threat-related files were downloaded.

- Web DLP analyzes data leaving your network to detect data exfiltration activity. Administrators can:
  - Create Web DLP policies that target the types of data loss activity that they want to monitor.
  - Use dashboard charts and incident reports in the Data Security manager to investigate data loss activity.

Installation

Topic 50632 | Release Notes | TRITON RiskVision | v7.8.1 | 22-Oct-2013

A Websense TRITON RiskVision deployment includes, at minimum:

- 1 Websense V5000 G2 or V10000 G3 appliance, hosting monitoring components

  All files required to activate TRITON RiskVision on the appliance are included on the appliance.
- 1 Windows Server 2008 R2 or Windows Server 2012 machine, hosting management and reporting components

  Get the Windows installer for TRITON RiskVision v7.8.0 from the Downloads page at mywebsense.com.

In addition, TRITON RiskVision components must be configured to connect to an existing Microsoft SQL Server 2008 or 2012 (standard, business intelligence, or enterprise) installation in your network.

Find basic setup instructions for the appliance in the Quick Start poster for the V5000 G2 and V10000 G3.

Refer to the Websense TRITON RiskVision Setup Guide for complete installation and configuration instructions.

After installation, see the Reporting Guide for tips about using reporting tools to verify and understand TRITON RiskVision monitoring and analysis.

Operating tips

Topic 50633 | Release Notes | TRITON RiskVision | v7.8.1 | 22-Oct-2013

TRITON RiskVision is an advanced traffic analysis tool used to investigate your organization's Internet activity. It does not block any Internet requests or responses.

By default, the only Internet monitoring policy configured for TRITON RiskVision applies the "permit" flag to all requests from all clients. In most deployments, no further policy configuration needs to be performed in the TRITON RiskVision manager.

In some circumstances, it may be desirable for administrators to configure policies that apply a "block" flag to some requests. Such policies are not used for enforcement.

Instead, they can be used to highlight types of Internet activity that are of interest to the organization in reports.

When you create policies that apply the “block” flag:

- If a policy “blocks” a request based on category or URL, the request is not sent to Content Gateway for analysis.
- Once a request receives the “block” flag, subsequent requests by the user for content internal to that website (for example, clicking through content on the site) may not appear in reports.

  This happens because TRITON RiskVision components do not know that the “block” is virtual. They act as though the user was stopped from viewing the website, and close the connection to the request.

Known issues

Topic 50634 | Release Notes | TRITON RiskVision | v7.8.1 | 22-Oct-2013

A list of known issues in this release is available to Websense TRITON RiskVision customers.

If you are not currently logged into MyWebsense, clicking the link brings up a login prompt. Log in to view the list.