



ThreatConnect® Risk Quantifier Release Notes

Software Versions 7.8 and 7.9

July 9, 2024



ThreatConnect® is a registered trademark of ThreatConnect, Inc.

FAIR™ is a trademark of The FAIR Institute.

CVE® and MITRE® are registered trademarks of The MITRE Corporation.



Table of Contents

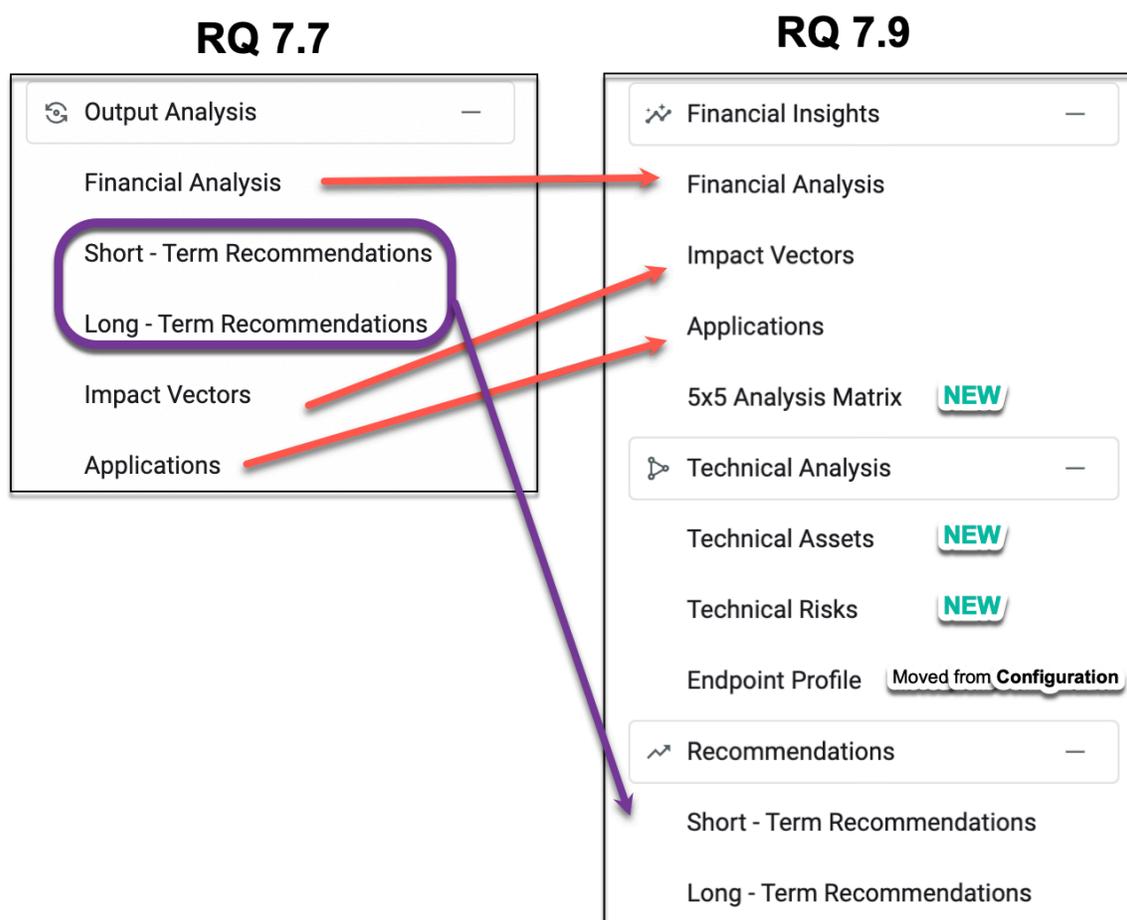
New Features and Functionality	4
Side Navigation Bar Updates	4
Heat Map: 5x5 Analysis Matrix	5
Technical Analysis	8
Technical Assets	8
Technical Risks	10
Endpoint Profile	10
Improvements	12
Integrations	14
Bug Fixes	15



New Features and Functionality

Side Navigation Bar Updates

In ThreatConnect Risk Quantifier (RQ) version 7.9, we replaced the **Output Analysis** option on the side navigation bar with three new options to help you access the information you are looking for more quickly and to include new features in this release.



Financial Insights includes the **Financial Analysis**, **Impact Vectors**, and **Applications** options previously found under **Output Analysis** and, for version 7.9, a new **5x5 Analysis Matrix** option. **Technical Analysis** includes two brand-new options—**Technical Assets** and **Technical Risks**—as well as the **Endpoint Profile** option previously found under **Configuration**. Finally, **Recommendations** includes the **Short-Term Recommendations** and **Long-Term Recommendations** options previously found under **Output Analysis**.

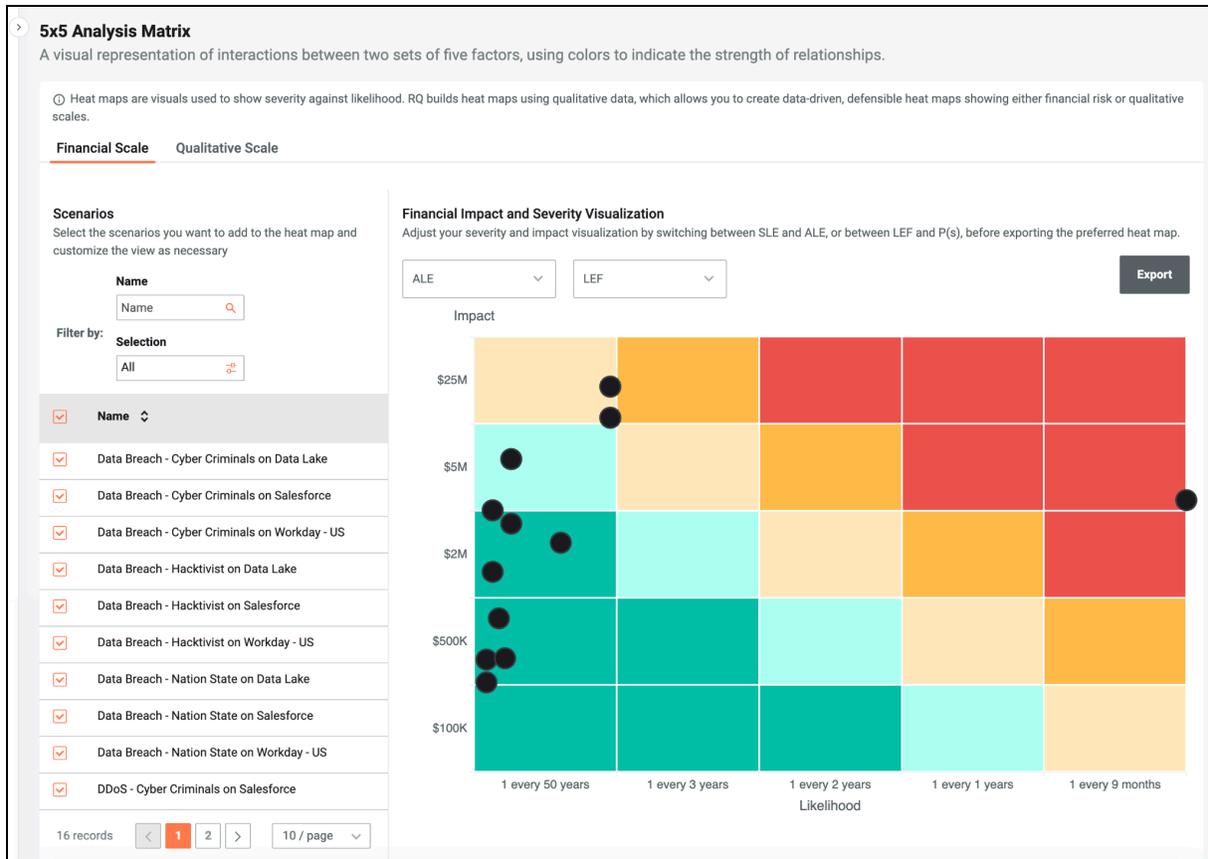


Heat Map: 5x5 Analysis Matrix

A common challenge our customers face is how to communicate financial risk to their business when they measure their risk qualitatively. Qualitative risk measures can be visualized in heat maps that show the impact and likelihood of a scenario. Unfortunately, heat maps tend to be subjective and lack data to back up their inputs.

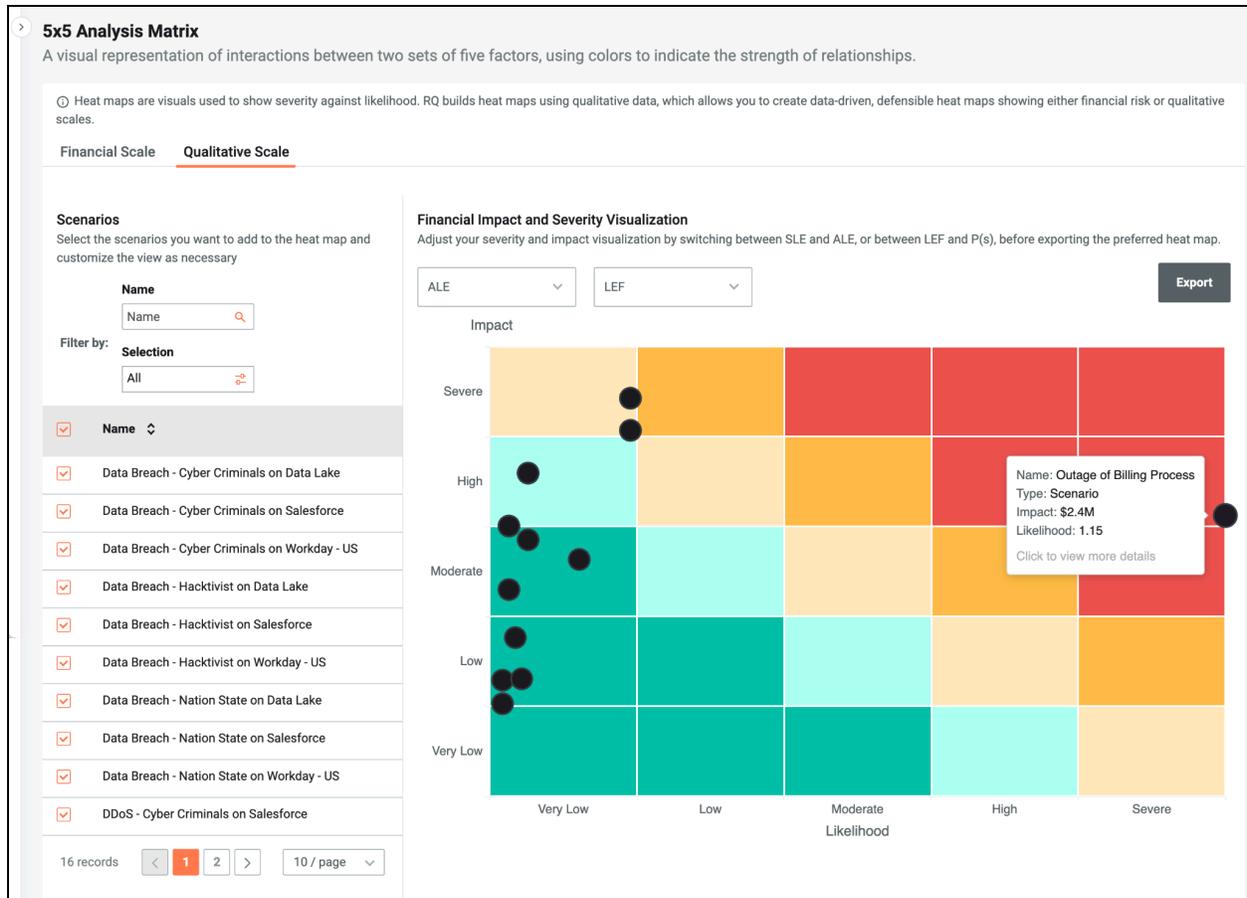
To address this gap, RQ 7.9 adds a data-driven heat map that shows scenarios calculated by RQ. The heat map can display financial scales or qualitative scales. For both scale types, you can choose to show the annualized loss expectancy (ALE) or single loss expectancy (SLE) on the y-axis and the P(s) (probability of an attacker succeeding) or loss event frequency (LEF) on the x-axis.

From the side navigation bar, select **5x5 Analysis Matrix** from the **Financial Insights** section. You will see a list of all scenarios for your Legal Entity, including Application and 'What If' scenarios, on the left and the heat map on the right. Select the **Financial Scale** or **Qualitative Scale** tab, and choose the scale for the y-axis and x-axis from the dropdowns above the heat map. Then select the checkbox for each scenario you want to include, or select the checkbox in the row header to add all scenarios. Each scenario is represented by a black dot on the heat map.



Financial-scale heat map

Hover over a dot to display a tooltip with information about its scenario. The tooltip shows the same information, including the scenario's financial impact and the likelihood for the selected axis types, on the **Financial Scale** and **Qualitative Scale** tab, providing a bridge between the two views. Click on the dot to display a window with more details about the scenario.



Qualitative-scale heat map showing a tooltip for one of the scenarios

Once you have built out your heat map, you can export it as a JPEG file by clicking **Export** at the upper right.

You can customize the labels for the qualitative scale and the financial ranges they correspond to in **Settings** → **Model Tuning** → **Qualitative Scale**.



Model Tuning
View and edit variables that are used in financial and probability calculations. Be aware that changing the default value will greatly impact the probability of loss and expected loss values.

Variables			
Loss Variables	Qualitative Scale		
Loss Limits	RQ lets you view outputs in financial terms or qualitative scales. Users can define their own qualitative scales below. The scales work on the heat map and other parts of RQ as well. The tables let you set values for showing loss magnitude (ALE or SLE, the scale will be used for both).		
CVE Weighting			
Annual Attack Rate of Incidence	Name	Lower Bound	Upper Bound
Fair - Primary Loss Magnitude Values	● Very Low ↗	\$0	\$100K ↗
Semi Automated FAIR Threat Event Frequency (TEF)	● Low ↗	\$100K ↗	\$500K ↗
Endpoint Score Weighting	● Moderate ↗	\$500K ↗	\$2M ↗
Qualitative Scale	● High ↗	\$2M ↗	\$5M ↗
	● Severe ↗	\$5M ↗	\$25M ↗

Customize the labels and ranges for the qualitative scale

Technical Analysis

The **Technical Analysis** section of the side navigation bar, introduced in RQ 7.8, includes three options in RQ 7.9:

- **Technical Assets:** Select any of your configured Applications and view technical risk information for each of its endpoints.
- **Technical Risks:** View all the potential Common Vulnerabilities and Exposures (CVE®s) for your enterprise and each CVE's Exploit Prediction Scoring System (EPSS) and Common Vulnerability Scoring System (CVSS) score and related information.
- **Endpoint Profile** (previously found under **Configuration**): View a summary of the endpoint configurations in your Legal Entity.

Technical Assets

A technical asset is a workstation, server, database, container, network device, or other piece of software or hardware that an attacker can latch onto in order to execute an action. In RQ, each technical asset receives a technical risk score from 0 to 1000, with 0 being the most secure and 1000 being the least secure. On the **Technical Assets** screen, you can select any of the Applications you have configured from the dropdown in the **What is my Target?**



section to view a list of the Application's technical assets (endpoints) and the technical risk for each technical asset in the **What is my Technical Risk?** section. Select a technical asset to view a summary of its information, an assessment of its technical risk score, and its CVE findings in the **What do I know about this Endpoint?** section.

Technical Assets
Cataloging endpoint profiles and libraries, identifying potential risks to organizational security.

Technical Assets List

What is my Target?
Select the application for which you want to view the technical risks.
Payments System

Application Details
Business Impact details about the current selected application.
Payments System
Single Loss Expectancy **\$63.6M**
Annual Loss Expectancy **\$5.9M**
Total Technical Assets **81**

What is my Technical Risk?
Technical Assets
Techniques are organized based on Financial Risk within the selected tactic.
Filter by: **Technical Risk Score** All

Technical Asset	IP Address	MAC Address	Technical Risk Score
BOS-DC-02	10.151.155.12	00:15:5d:98:ff:01	847
10.151.154.10	10.151.154.10	Unknown	847
BOS-VHOST-02	10.151.154.12	18:66:da:90:90:a9	846
172.31.51.216	Unknown	Unknown	812
ubuntu server	Unknown	Unknown	812
10.151.154.6	10.151.154.6	Unknown	808
10.151.152.101	10.151.152.101	Unknown	795
amazon linux 2 - web...	Unknown	Unknown	607
10.151.152.10	10.151.152.10	Unknown	221
14:18:77:60:c3:29	10.151.156.6	14:18:77:60:c3:29	195

81 records

What do I know about this Endpoint?

Endpoint Information
Technical Asset: **amazon linux 2 - webgoat**
OS Platform: **Unknown**
Source: **AppSec**
IP Address: **Unknown**
MAC Address: **Unknown**

Technical Risk Score
High Risk
607

Subscores
Vulnerability: 65 N/A
Application Security: 1000

Findings
CVE Findings: 1
CVE findings refer to the discoveries or reports of vulnerabilities and exposures in software, hardware, or systems that have been assigned CVE identifiers.
View All Findings

View technical risk scores for an Application's technical assets (endpoints)

RQ uses four analysis factors when computing an endpoint's technical risk score:

- Vulnerability data
- Application security data
- Subnet analysis
- Partner scoring

Endpoint technical risk scores are used when evaluating CVEs on the **Short-Term Recommendations** screen.



Technical Risks

The **Technical Risks** screen lists the potential CVEs in your enterprise's environment. For each CVE, it provides the following information, which is used to calculate the technical risk score for your Legal Entity's technical assets:

- The CVE's EPSS score and exploitability ranking
- The CVE's CVSS score, date of publication, and last asset date as provided by the National Institute of Standards and Technology's [National Vulnerability Database \(NVD\)](#)

Technical Risks					
A comprehensive inventory of potential technical vulnerabilities and challenges, curated to safeguard enterprise operations.					
Technical Risks List					
CVE	EPSS Score	EPSS Exploitability	CVSS Score	Published Date	Last Asset Date
Filter by: CVE	All	All	All	All	All
What are my Technical Risks?	Exploit prediction scoring system (EPSS)		Common Vulnerability Scoring System (CVSS)		
CVE-2021-45105	EPSS Score: 96.62%	EPSS Exploitability: 1	CVSS Score: 5.9	Published Date: December 18, 2021 6:55 AM	Last Asset Date: July 25, 2022 12:41 PM
CVE-2021-20304	EPSS Score: 0.22%	EPSS Exploitability: 0.6	CVSS Score: 7.5	Published Date: August 22, 2022 8:00 PM	Last Asset Date: October 30, 2022 8:00 PM
CVE-2021-37576	EPSS Score: 0.1%	EPSS Exploitability: 0.4	CVSS Score: 7.8	Published Date: July 26, 2021 5:35 PM	Last Asset Date: September 25, 2021 10:06 AM

View CVE data used to calculate technical risk scores for your technical assets

You can click on a CVE to view its details in the NVD. You can also view more information about each CVE on [MITRE®'s CVE Program website](#).

Endpoint Profile

The **Endpoint Profile** screen, previously found under **Configuration**, displays an analysis of the endpoints for the Applications configured in your Legal Entity.



Endpoint Profile

Endpoint Profiles are patterns of server and endpoint configurations that are found across your legal entity. The default profile will be applied automatically to all the Applications you create.

Servers Workstations

81 6

You have the option to delete all your current endpoints and create new ones if needed. However, please note that this action is permanent.

Delete All Endpoints

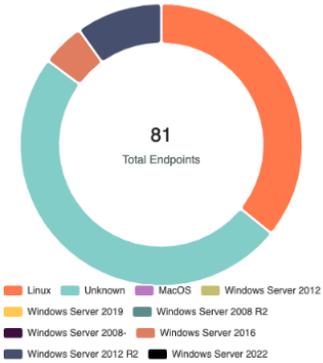
Distribution by Operating System

Below is the target endpoints distribution based on Operating Systems. The number is based on data ingested from scans provided in Integrations.

Operating System	Distribution of Endpoints	Number of Endpoints
Linux	35.8%	29
Unknown	49.38%	40
MacOS	0%	0
Windows Server 2012	0%	0
Windows Server 2019	0%	0
Windows Server 2008 R2	0%	0
Windows Server 2008-	0%	0
Windows Server 2016	4.94%	4
Windows Server 2012 R2	9.88%	8
Windows Server 2022	0%	0

Distribution by Operating System Chart

Distribution of target endpoints (i.e., endpoints used for storing data and/or involved in transaction processing) this profile has in place. The default data is based on scans provided in Integrations.



View an analysis of the endpoint configurations in your Legal Entity



Improvements

- On the **Financial Analysis** screen in RQ 7.9, **Lower Bound** and **Upper Bound** columns were added to the **RQ-ALE** section of the **Loss Breakdown by Type and Application** table.

Financial Analysis
Below is a detailed view of your Financial Risk Analysis. Depending on data relevance, charts display either RQ-SLE, RQ-ALE or both.🌐

Loss Breakdown by Type and Application							RQ-SLE	RQ-ALE	Search
Attack									
Filter by: Data Breach									
Applications	How we compute this	Remediation	Legal	Settlement	Per Record Flat Fees	GDPR Fines	RQ-ALE		
							Lower Bound	Total	Upper Bound
	Data Lake	\$1.2M	\$1M	\$7.5M	\$2.6M	\$1.2M	\$3.6M	\$13.5M	\$51.6M
	Salesforce	\$1.2M	\$1M	\$7.5M	\$2.6M	\$1.2M	\$3.6M	\$13.5M	\$51.6M
	Workday - US	\$1.2M	\$1M	\$4M	\$92.1K	\$0	\$3.6M	\$6.4M	\$36M

- When viewing a **Model risk to business assets** 'What If' analysis in RQ 7.8 and 7.9, there is now a **Total** row in the **Financial Analysis** table.

Financial Analysis

Loss Type	Minimum	Most Likely	Maximum
Remediation	\$4.1M	\$4.1M	\$17.9M
Per Record Flat Fees	\$17.2K	\$369.3K	\$73.8M
GDPR Fines	\$24.7K	\$2.4M	\$31.2M
Settlement	\$7.5M	\$10.4M	\$26.1M
Legal	\$669.8K	\$906.1K	\$3.4M
Total	\$12.3M	\$18.2M	\$152.4M

- When viewing a **FAIR Scenario** 'What If' analysis in RQ 7.9, the **Characteristics of the loss** table now includes rows for 10%, 25%, 50%, 75%, 90%, and 95%.



Characteristics of the loss	
Risk's characteristics	ALE
Minimum	\$131.7K
10%	\$516.2K
25%	\$939.4K
50%	\$1.7M
Average	\$2.4M
75%	\$3.3M
90%	\$5.3M
95%	\$6.5M
Maximum	\$11.2M



Integrations

ThreatConnect RQ has added the following integrations:

- **Windows Defender:** This integration is used to analyze technical risks to endpoints.



Bug Fixes

- Resolved issues preventing some notifications for custom tables from being displayed in the **Notifications** section.
- Corrected issues related to the reconciliation of CVEs and endpoints.
- Enhanced performance for short-term recommendations, particularly when handling a large number of CVEs in the database.
- Fixed issues with the Data Export API where multi-control profile (MCP) scenarios were causing a 500 error due to invalid inputs in the payload.
- Addressed an issue with Single Sign-On (SSO) that was preventing updates to provider names.
- Rectified an issue in FAIR™ scenarios by setting a limit of 3000 characters on certain fields.
- Implemented several fixes for the AppSoc integration.