ThreatConnect® Risk Quantifier Release Notes

Software Version 7.0

March 31, 2023

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: 703.229.4489
www.ThreatConnect.com

Table of Contents

New Features and Functionality

New Control Types

Control frameworks such as NIST CSF, CIS 18, and ISO 27001 help organizations understand and measure the performance of their security program. Each framework consists of controls that describe the technical environment, people, and processes required to secure an organization.

ThreatConnect® Risk Quantifier (RQ) uses control assessments to calculate the likelihood of an attacker overcoming an organization's defenses. RQ Version 7.0 changes how the platform looks at controls by splitting them into three types:

- Technical controls
- Loss controls
- Amplification controls

Technical controls operate by resisting an attacker's actions, narrowing the focus of what an attacker can achieve while reducing the likelihood that any given action will be successful.

Loss controls directly influence the loss magnitude (i.e., single loss event [SLE]) of an attack and help mitigate the effects of a successful attack.

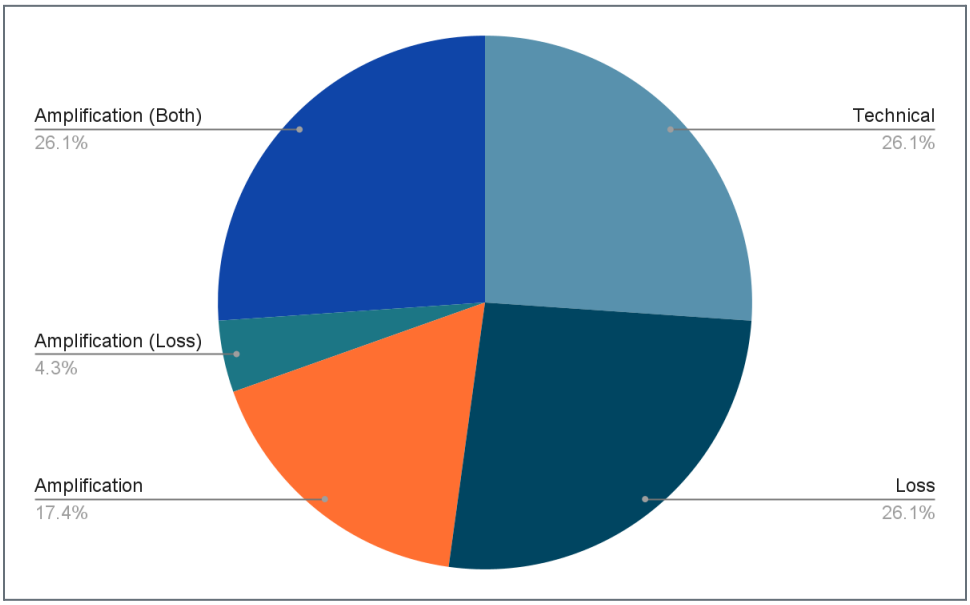
Amplification controls are designed to cover activities that increase or decrease the effectiveness of other controls. These controls do not block an attacker's actions, nor do they directly help with mitigating losses; instead, they indicate increasing confidence in the consistency, universality, and scope of the configuration for other controls. Amplification controls can apply to loss controls, technical controls, or both.

As an example, NIST CSF is a strategic framework with 23 controls across 5 categories. The following table illustrates how RQ categorized those 23 controls as Technical, Loss, and Amplification controls.

Technical	Loss	Technical Amplification	Loss Amplification	Technical & Loss Amplification	Total Control Count
6	6	4	1	6	**23**

Count of controls in each category

The following chart shows the percentage that each control type comprises in RQ Version 7.0 for NIST CSF.



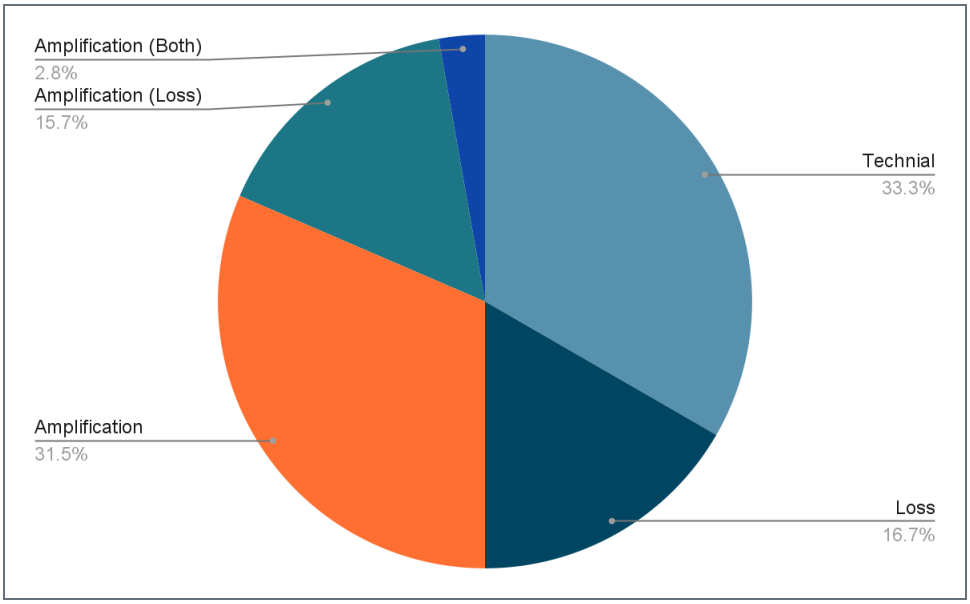
Percentage of controls in each category for NIST CSF

At the subcategory level, the strategic nature of NIST CSF is more pronounced. This leads to a higher percentage of amplification controls, as detailed in the following table.

Technical	Loss	Technical Amplification	Loss Amplification	Technical & Loss Amplification	Total Control Count
36	18	34	17	3	**108**

Count of subcontrols in each category

The following chart shows the percentage each control type comprises in RQ Version 7.0 for NIST CSF with subcontrols.



Percentage of controls in each category for NIST CSF with subcontrols

A similar analysis is available for each security framework, the results of which will be displayed in RQ with the appropriate labels.

Updated Loss Models

RQ Version 7.0 includes updated loss models based on advanced research techniques. The new models are more highly tuned and attenuated to current losses and represent a new set of techniques for modeling cyber losses.

In addition, RQ Version 7.0 will now show the median value for "computed loss" instead of the 80% value that was shown in Version 6.7. Median is defined as the value in the middle of a data set, meaning that 50% of data points have a value smaller or equal to the median and 50% of data points have a value higher or equal to the median. The change to show median values was made because it is a more accurate representation of an interval midpoint that is not affected by outliers or other extreme values. The new losses in RQ, which were computed using updated models, include outputs that are point estimates alongside a confidence range, with the most likely value being computed as the median of those outputs.

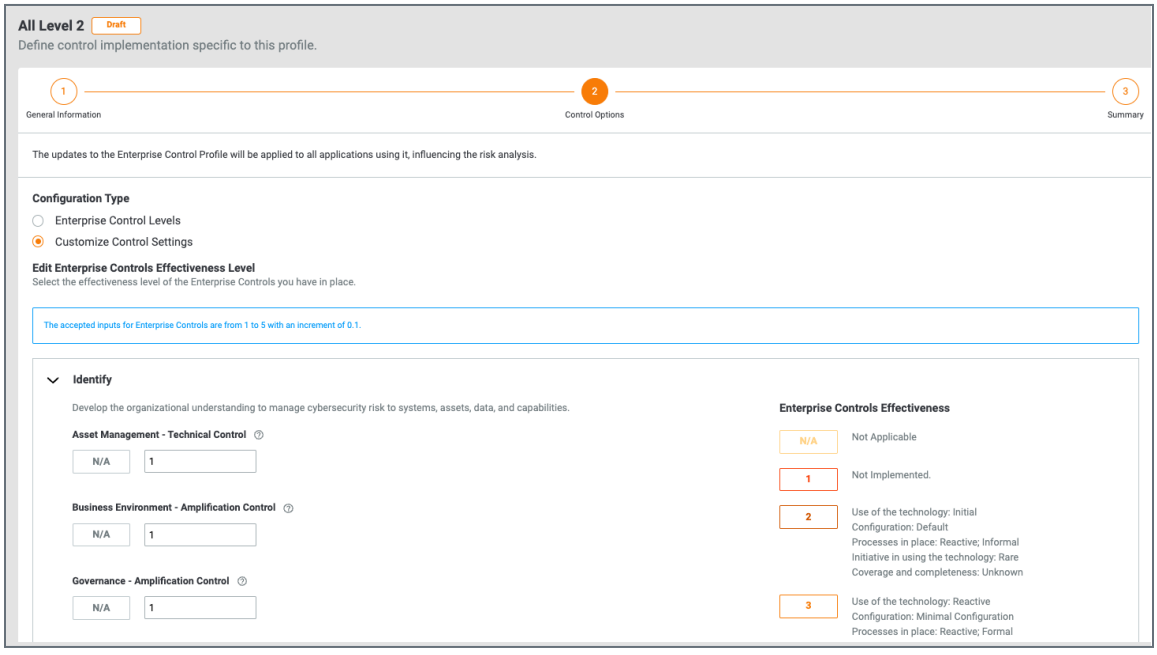
New Settlement Loss Type

RQ Version 6.7 categorized all legal costs related to a data breach as one loss type: **Legal**. RQ Version 7.0 splits the settlement costs and other legal costs into two loss types: **Settlement** and **Legal**. The Settlement loss type covers the values due after all legal actions are complete, whereas the Legal loss type incorporates legal fees sustained.

Legal and Settlement are shown as two separate loss types

Decimal Values for Control Profiles

Occasionally, customers assess the maturity of their controls in decimal values instead of whole numbers. For example, a customer using the NIST CSF framework may have assessed the maturity of their Asset Management capability as 2.5 (instead of 2 or 3). In RQ Version 7.0, users can now enter maturity values for Control Profiles in decimal format.

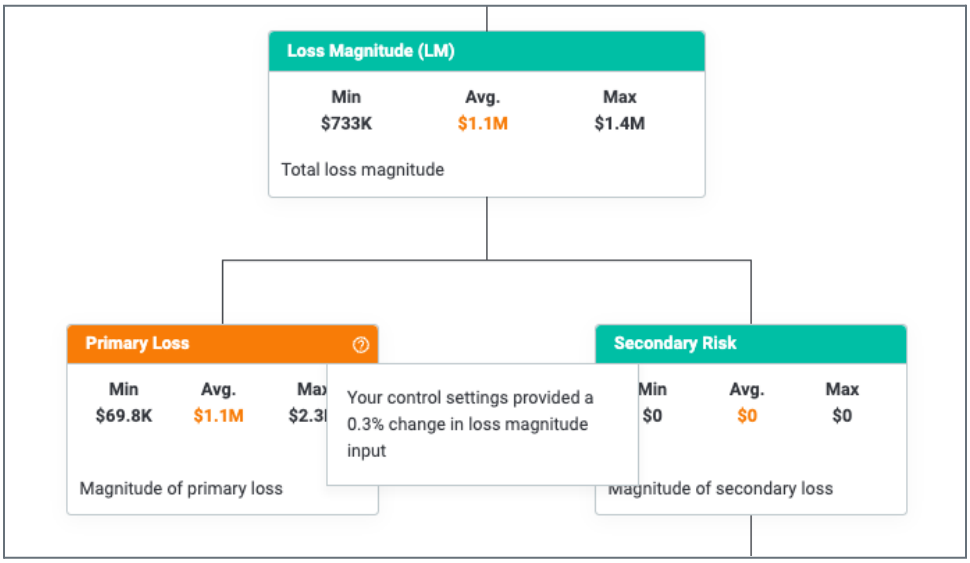


Control Profiles now accept values in decimal format

Changes to Semi-Automated FAIR Outputs

Semi-automated FAIR™ (SAF) scenarios leverage the new control schemes outlined in the "New Control Types" section, resulting in two key changes to the outputs for these scenarios.[1]

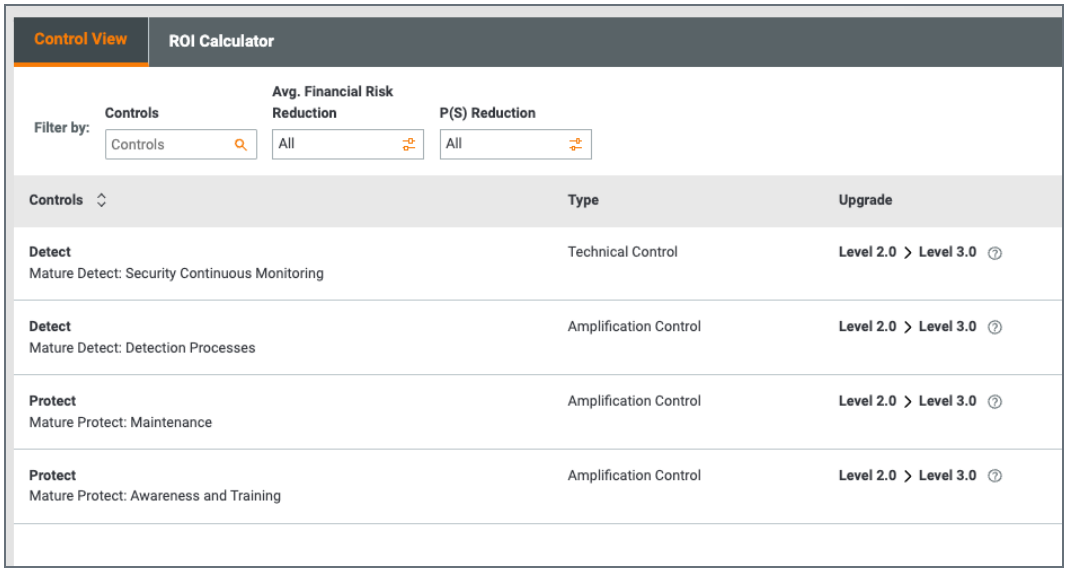
When viewing SAF scenario outputs, RQ now shows the impact of loss controls via a tooltip that is displayed when you click the **?** icon next to **Primary Loss** heading. Loss controls apply to the magnitude of a loss, which corresponds to the "Primary Loss" values in FAIR; they do not apply to secondary losses.



Tooltip showing the impact of loss controls for Primary Loss

In addition, a **Type** column that denotes each control's type will be displayed on the **Control View** tab of SAF outputs.

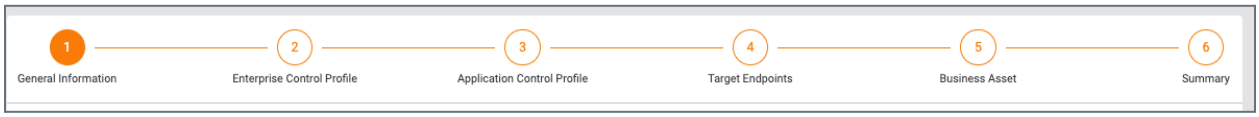
[1] FAIR™ is a trademark of The Fair Institute.



SAF output showing the new control types

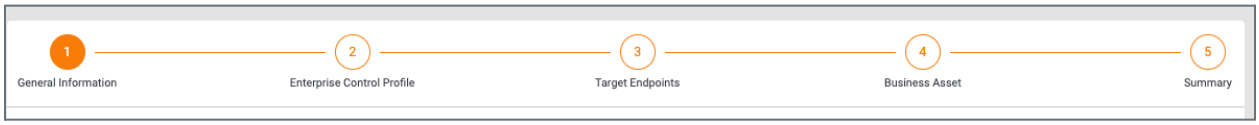
Updates to Business Applications and Removal of Application Controls

In RQ Version 6.7, users could create Application Controls that represented a refinement of Enterprise Controls and had a minor impact on the probability calculations.



Business Application Creation with Application Controls in RQ Version 6.7

As of RQ Version 7.0, you will no longer be able to create Application Controls. However, standard mechanisms for control refinement, including ingesting endpoint data and application security data, will be added in future releases.



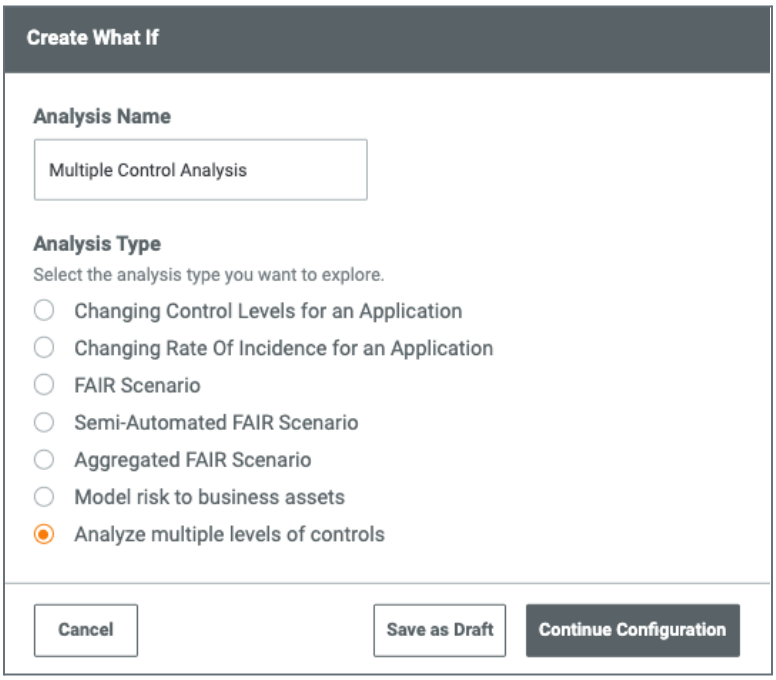
Business Application Creation without Application Controls in RQ Version 7.0

Compare Multiple Control Profiles

Many customers use RQ to compare three possible configurations for their environments:

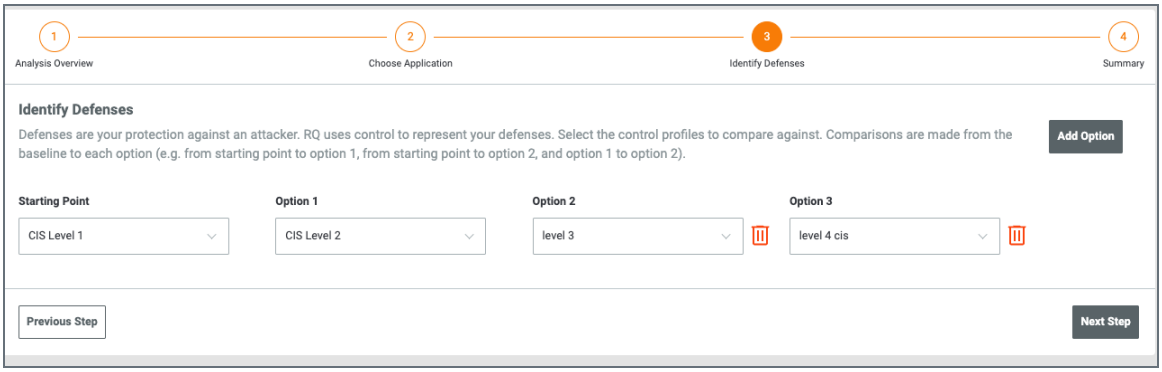
- No controls (there are no controls in the environment)
- Actual state (where controls are today)
- Desired state (where controls should be based on desired risk levels)

This required customers to create multiple Business Applications and run several calculations to generate the comparisons. To streamline this effort for customers, RQ Version 7.0 introduces a new analysis type for "What If" scenarios: **Analyze multiple levels of controls**.



Analyzing multiple levels of controls using a "What If" scenario

After selecting **Analyze multiple levels of controls** as the analysis type, users can choose an Application and then identify which Control Profiles to compare. Users *must* select a **Starting Point** Control Profile, followed by the Control Profiles they want to use in the comparison.

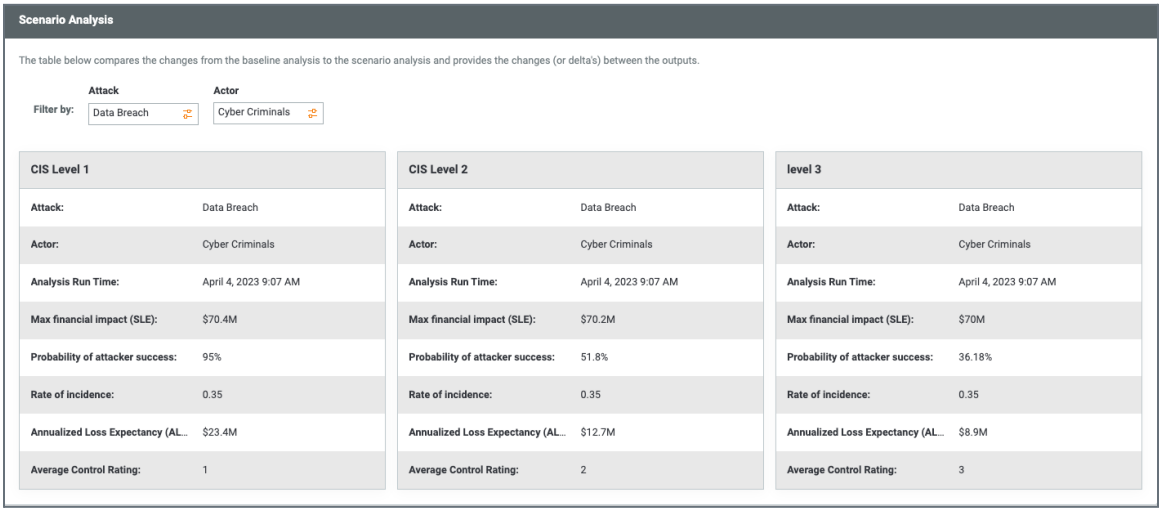


Selecting Control Profiles to compare

RQ will compute the difference between all combinations of Control Profiles from left to right. In the preceding image, four possible Control Profiles are shown. When this "What If" scenario runs, RQ will compute the difference between the four Control Profiles as follows:

- Starting Point and Option 1
- Starting Point and Option 2
- Starting Point and Option 3
- Option 1 and Option 2
- Option 1 and Option 3
- Option 2 and Option 3

After the “What If” scenario finishes running, you can view the results of the comparisons performed during the analysis.



Results of “What If” scenario comparing multiple Control Profiles

Removal of Market Impact

In RQ Version 6.7, reputation data was categorized as Market Impact. As of RQ Version 7.0, Market Impact was removed from the platform as new models for reputation are being developed. This means that the **Market Impact** screen is no longer available, and the following fields will no longer be displayed when configuring a Legal Entity:

- **How many customers does the legal entity have?**
- **What was the average value of a customer over the last fiscal year?**
- **What is the projected customer growth rate for the current fiscal year?**

Bug Fixes

The following bug fixes were applied to the 7.0 RQ release:

- An issue causing performance issues to occur when running risk analyses was fixed.
- An issue preventing semi-automated FAIR scenarios from running due to unmatched encryption keys was fixed.