ThreatConnect® Risk Quantifier Release Notes

Software Version 7.7

February 28, 2024

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

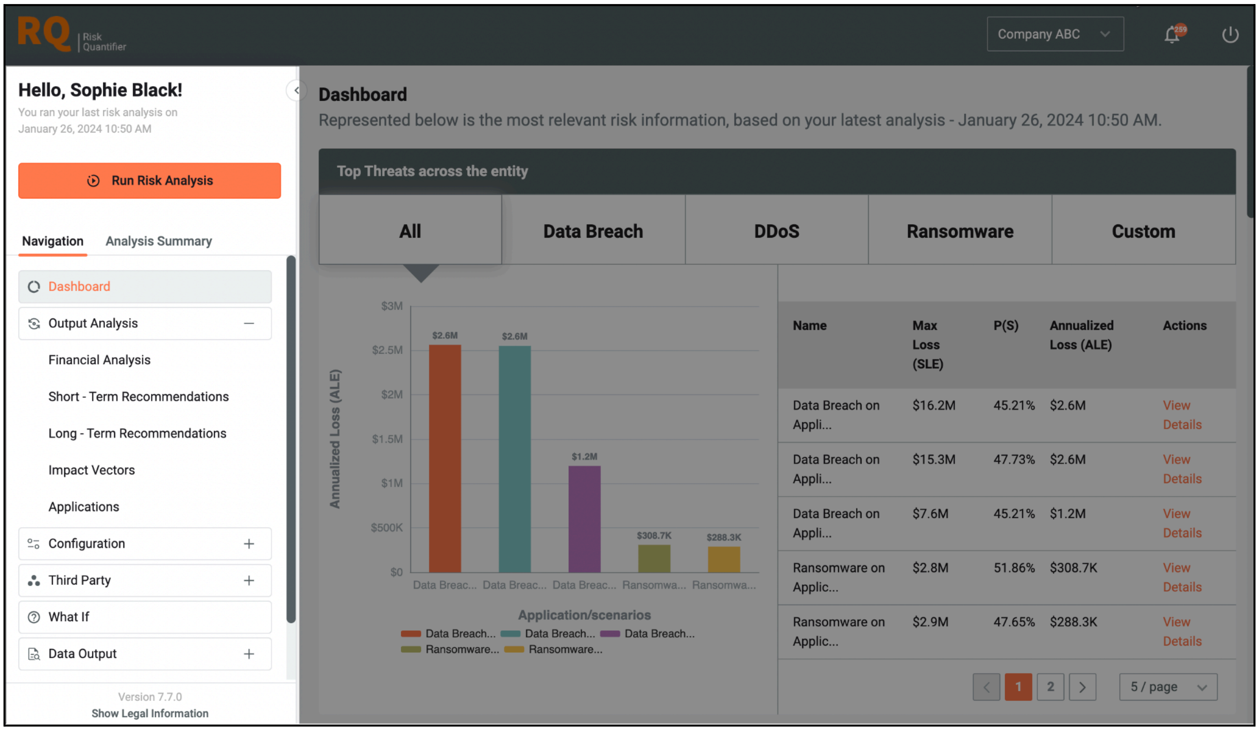
P: 1.800.965.2708 I F: 703.229.4489
www.ThreatConnect.com

Table of Contents

New Features and Functionality

New Navigation Bar and Analysis Summary

ThreatConnect® Risk Quantifier (RQ) version 7.7 debuts a streamlined new look that provides easy access to all the main features of the platform from a side navigation bar instead of a top navigation bar. Most of the navigation bar options are dropdowns that can be expanded to display the names of all available screens provided by the option.



Hello, Sophie Black!

You ran your last risk analysis on January 26, 2024 10:50 AM

Dashboard

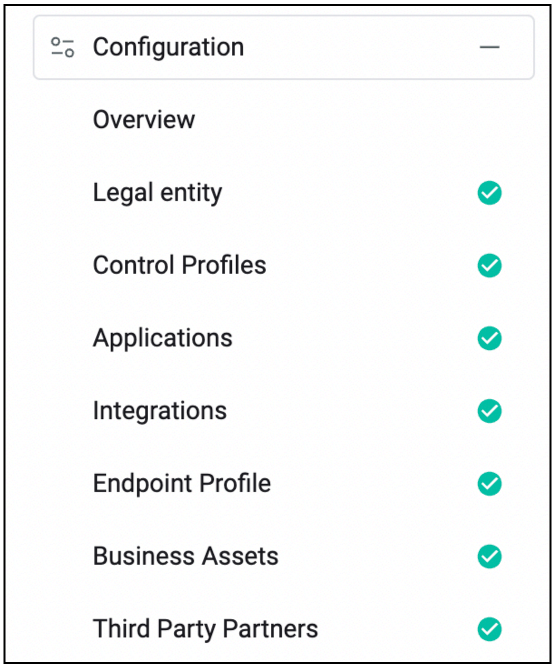
Represented below is the most relevant risk information, based on your latest analysis - January 26, 2024 10:50 AM.

Name	Max Loss (SLE)	P(S)	Annualized Loss (ALE)	Actions
Data Breach on Appli...	$16.2M	45.21%	$2.6M	View Details
Data Breach on Appli...	$15.3M	47.73%	$2.6M	View Details
Data Breach on Appli...	$7.6M	45.21%	$1.2M	View Details
Ransomware on Applic...	$2.8M	51.86%	$308.7K	View Details
Ransomware on Applic...	$2.9M	47.65%	$288.3K	View Details

The new side navigation bar has expandable options for all available screens

Note: The dropdown for toggling between portfolio view and Legal Entities in the Enterprise is still available to RQ Enterprise users at the top right of the screen.

When expanded, the **Configuration** option lists all configuration screens, as well as an indication of whether the configuration on each screen has been completed.



Configuration —

Overview

Legal entity ✓

Control Profiles ✓

Applications ✓

Integrations ✓

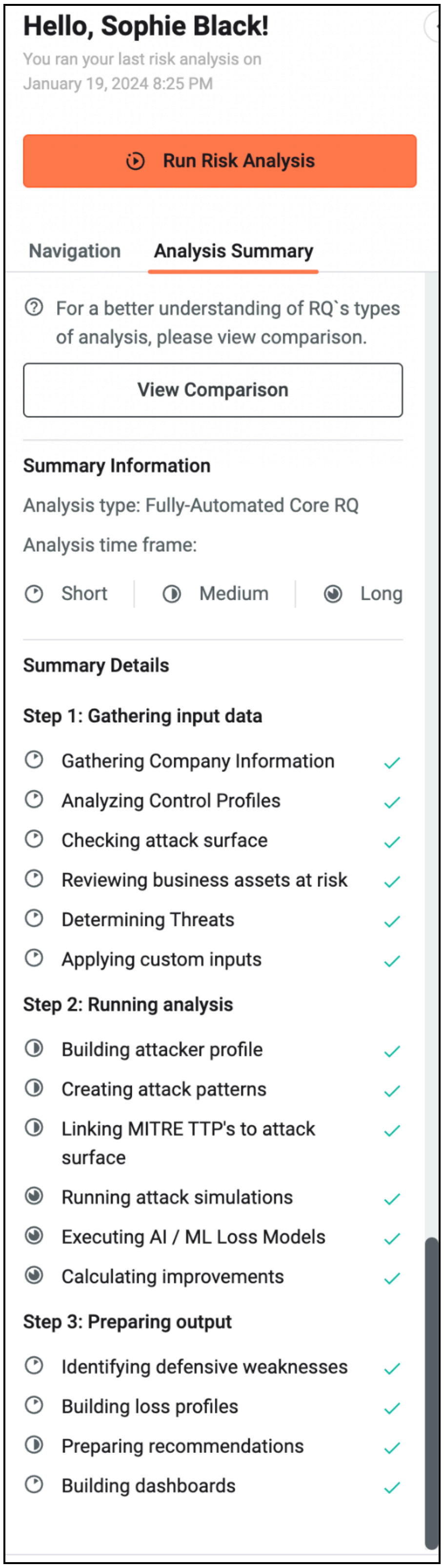
Endpoint Profile ✓

Business Assets ✓

Third Party Partners ✓

*The **Configuration** option lists each screens and whether its configuration is complete*

In addition, the new side navigation bar provides an **Analysis Summary** tab that lists the steps for your selected type of risk analysis.



Hello, Sophie Black!

You ran your last risk analysis on January 19, 2024 8:25 PM

For a better understanding of RQ`s types of analysis, please view comparison.

Summary Information

Analysis type: Fully-Automated Core RQ

Analysis time frame:

Short | Medium | Long

Summary Details

Step 1: Gathering input data

- Gathering Company Information ✓
- Analyzing Control Profiles ✓
- Checking attack surface ✓
- Reviewing business assets at risk ✓
- Determining Threats ✓
- Applying custom inputs ✓

Step 2: Running analysis

- Building attacker profile ✓
- Creating attack patterns ✓
- Linking MITRE TTP's to attack surface ✓
- Running attack simulations ✓
- Executing AI / ML Loss Models ✓
- Calculating improvements ✓

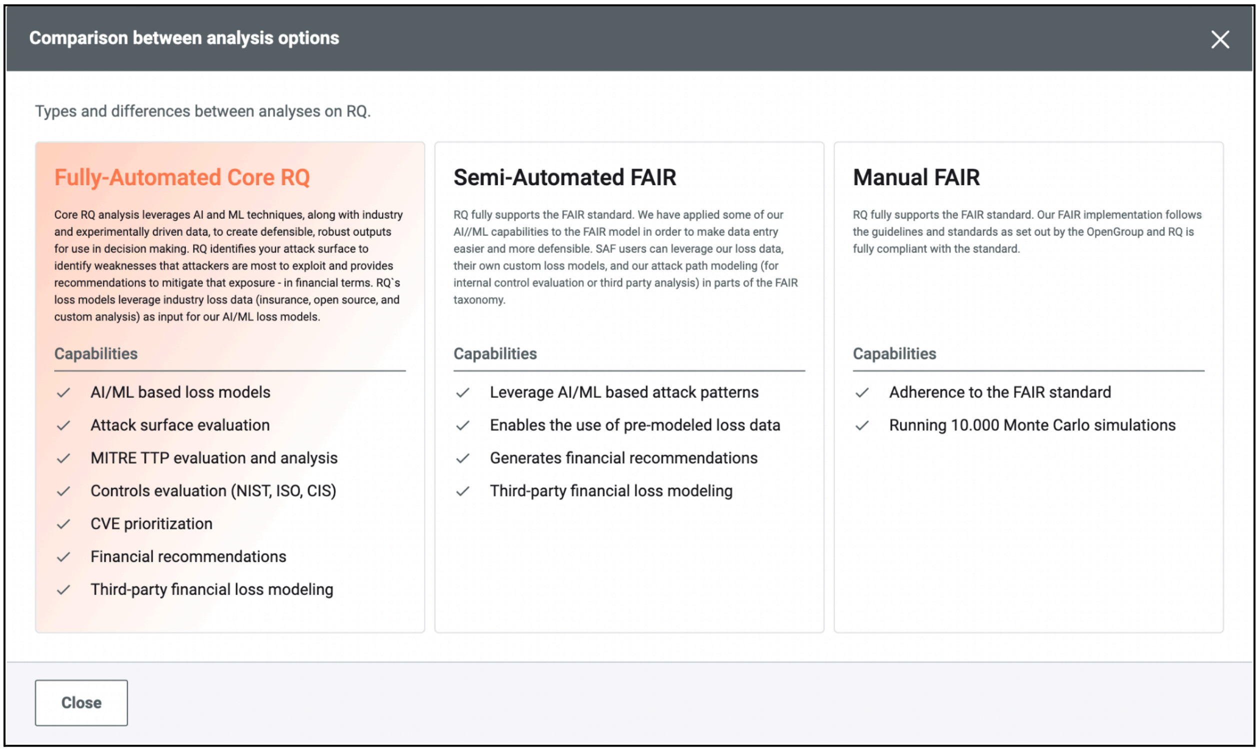
Step 3: Preparing output

- Identifying defensive weaknesses ✓
- Building loss profiles ✓
- Preparing recommendations ✓
- Building dashboards ✓

*The **Analysis Summary** tab displays the steps for your risk analysis*

When you click **Run Risk Analysis** above the navigation bar, the **Summary Details** section of the **Analysis Summary** will reset, showing in real time whether each step has been completed as the analysis runs and then remaining as a record of all of the steps that were taken for the analysis.

Click the **View Comparison** button to view a window displaying a summary of each risk analysis type.



Comparison between analysis options

Types and differences between analyses on RQ.

Fully-Automated Core RQ

Core RQ analysis leverages AI and ML techniques, along with industry and experimentally driven data, to create defensible, robust outputs for use in decision making. RQ identifies your attack surface to identify weaknesses that attackers are most to exploit and provides recommendations to mitigate that exposure - in financial terms. RQ`s loss models leverage industry loss data (insurance, open source, and custom analysis) as input for our AI/ML loss models.

Capabilities

- ✓ AI/ML based loss models
- ✓ Attack surface evaluation
- ✓ MITRE TTP evaluation and analysis
- ✓ Controls evaluation (NIST, ISO, CIS)
- ✓ CVE prioritization
- ✓ Financial recommendations
- ✓ Third-party financial loss modeling

Semi-Automated FAIR

RQ fully supports the FAIR standard. We have applied some of our AI//ML capabilities to the FAIR model in order to make data entry easier and more defensible. SAF users can leverage our loss data, their own custom loss models, and our attack path modeling (for internal control evaluation or third party analysis) in parts of the FAIR taxonomy.

Capabilities

- ✓ Leverage AI/ML based attack patterns
- ✓ Enables the use of pre-modeled loss data
- ✓ Generates financial recommendations
- ✓ Third-party financial loss modeling

Manual FAIR

RQ fully supports the FAIR standard. Our FAIR implementation follows the guidelines and standards as set out by the OpenGroup and RQ is fully compliant with the standard.

Capabilities

- ✓ Adherence to the FAIR standard
- ✓ Running 10.000 Monte Carlo simulations

*Click **View Comparison** to view a summary of each risk analysis type*

RQ Impacts

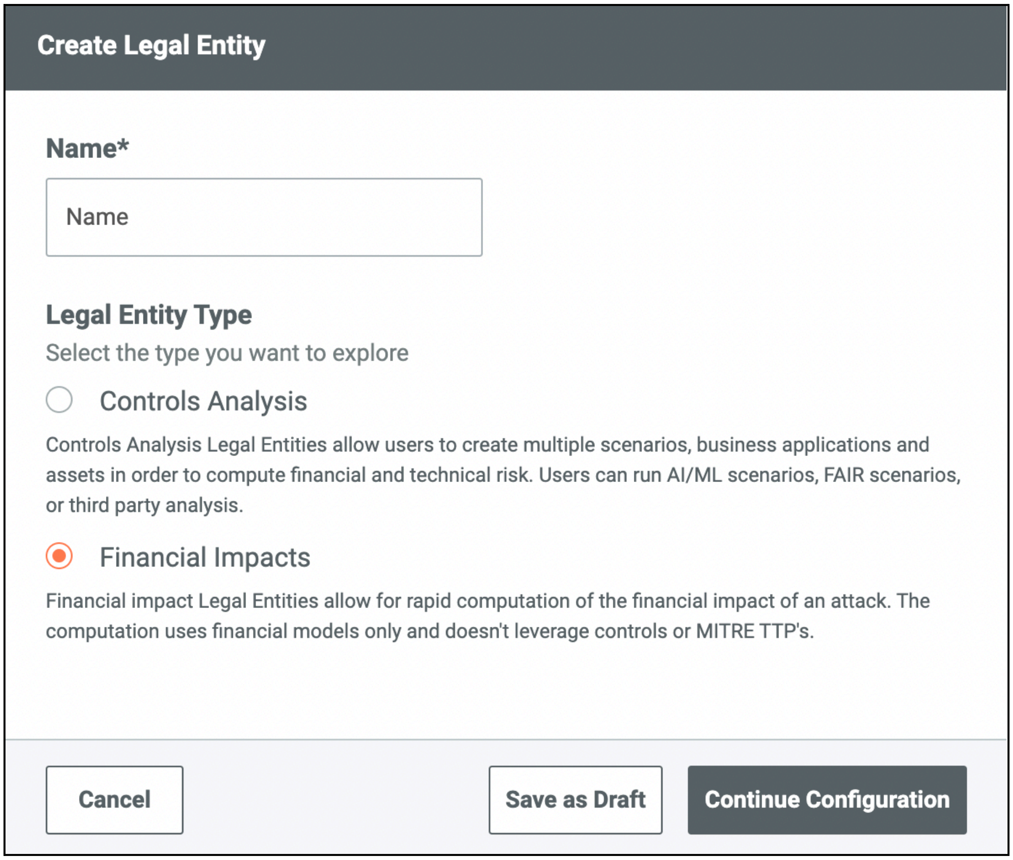
Version 7.7 debuts a new product, RQ Impacts, a lightweight version of ThreatConnect RQ that rapidly computes a set of potential loss impacts based on your organization's revenue and number of data records at risk. It quickly computes, with minimal inputs and configuration, the financial impact of an attack against your organization. The analysis provides two types of results:

- your organization's material financial risks as defined by the U.S. Securities and Exchange Commission's (SEC's) concept of materiality

- the information you would need to calculate cyber insurance amounts for 50%, 80%, 90%, 95%, and 99% loss levels

RQ Impacts is essentially a “lite” version of ThreatConnect RQ that rapidly shows you what your loss impacts could be based on the amounts of revenue and data at risk that you provide. These calculations are made on the basis of peer analytics, enabling you to validate and confirm that the risks your company faces are being realized by companies in your industry with a similar amount of revenue or companies that have experienced similar losses to those that your company could face.

You can access RQ Impacts via a new type of Legal Entity: **Financial Impacts**. If you have purchased only the RQ Impacts product, then **Financial Impacts** will be the only available Legal Entity type. All other RQ customers will be able to access the **Financial Impacts** Legal Entity type as well as the original Legal Entity type, now called **Controls Analysis**.



Create Legal Entity

Name*

Name

Legal Entity Type

Select the type you want to explore

○ Controls Analysis

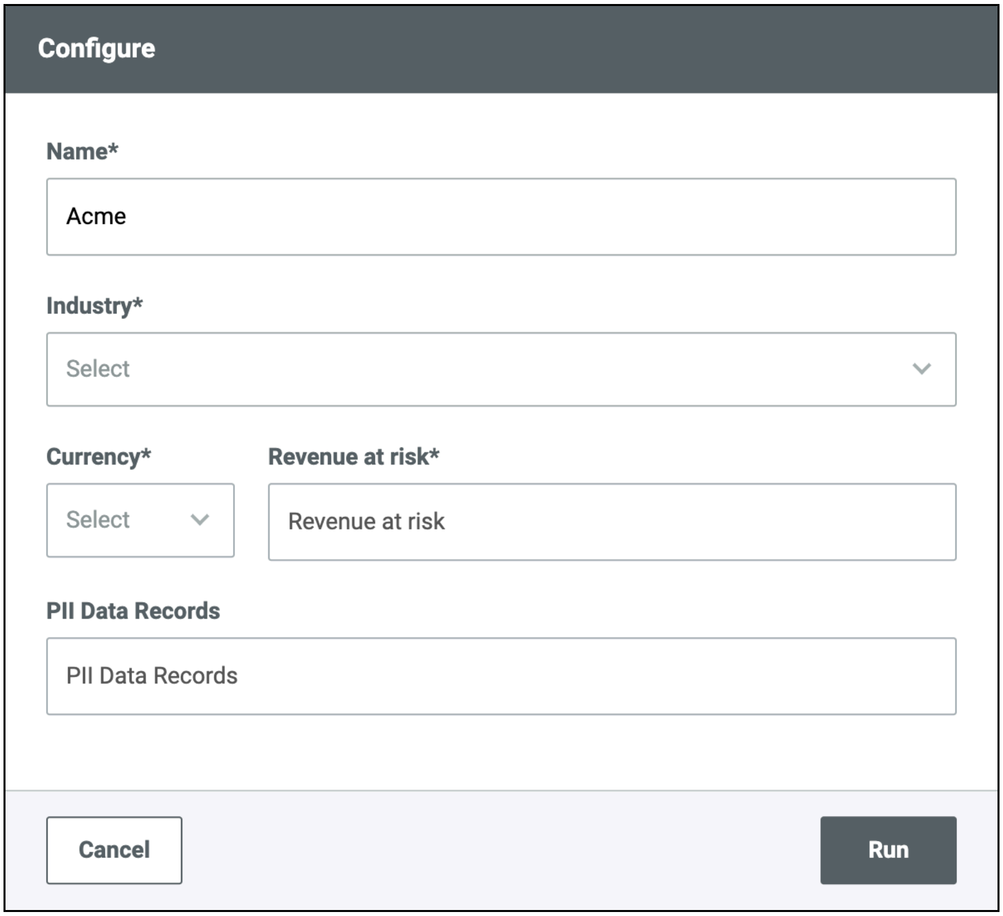
Controls Analysis Legal Entities allow users to create multiple scenarios, business applications and assets in order to compute financial and technical risk. Users can run AI/ML scenarios, FAIR scenarios, or third party analysis.

● Financial Impacts

Financial impact Legal Entities allow for rapid computation of the financial impact of an attack. The computation uses financial models only and doesn't leverage controls or MITRE TTP's.

*Select the **Financial Impacts** Legal Entity type to use RQ Impacts*

In the configuration for your **Financial Impacts** Legal Entity, you will be prompted to enter only a few pieces of information.



Configure

Name*

Acme

Industry*

Select

Currency*

Select

Revenue at risk*

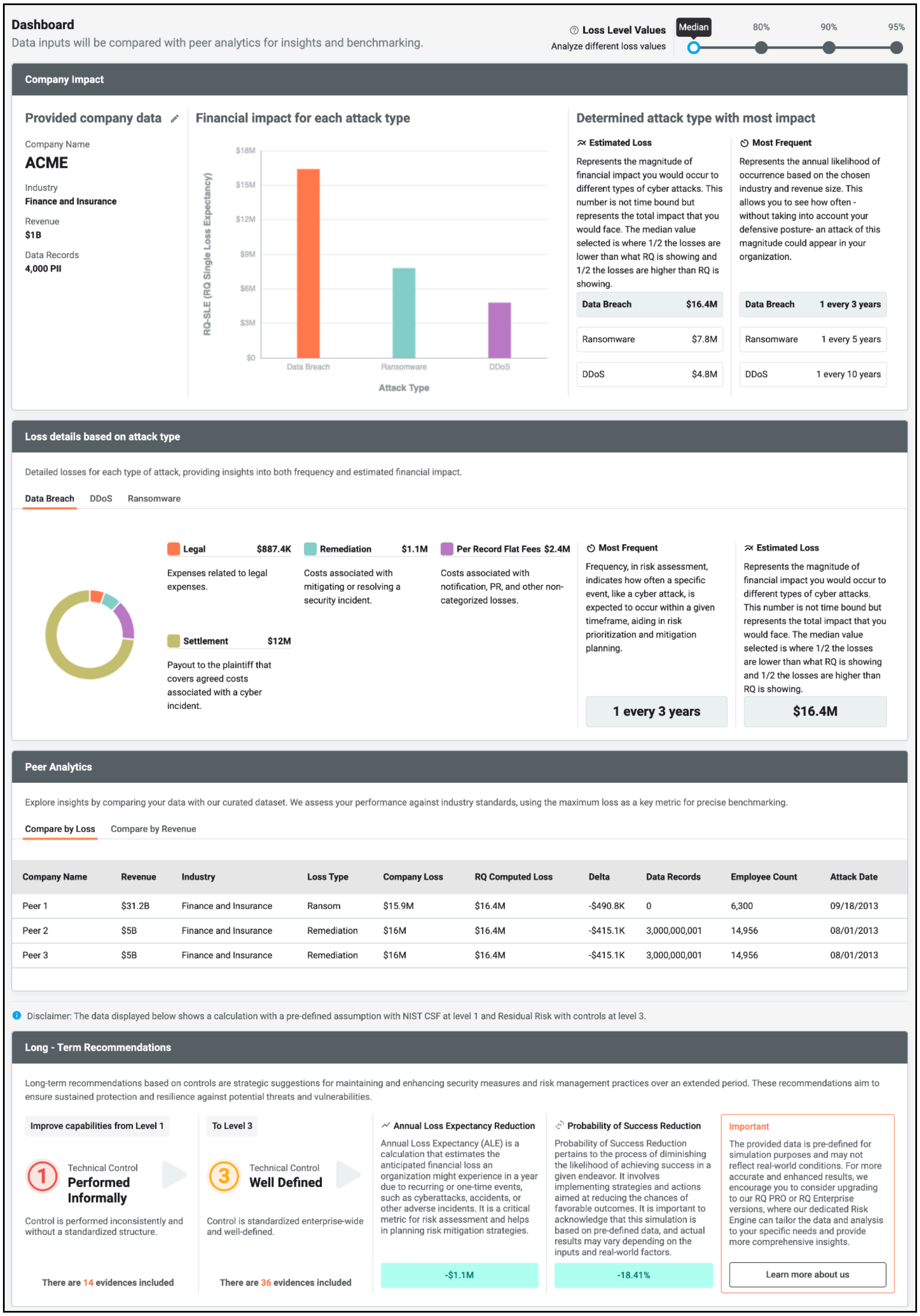
Revenue at risk

PII Data Records

PII Data Records

*Configuration of a **Financial Impacts** Legal Entity is quick and easy*

The data model will then run the risk analysis and display a dashboard showing the results.



Dashboard

Data inputs will be compared with peer analytics for insights and benchmarking.

Company Impact

Provided company data

Company Name
ACME

Industry
Finance and Insurance

Revenue
$1B

Data Records
4,000 PII

Financial impact for each attack type

Determined attack type with most impact

Estimated Loss

Represents the magnitude of financial impact you would occur to different types of cyber attacks. This number is not time bound but represents the total impact that you would face. The median value selected is where 1/2 the losses are lower than what RQ is showing and 1/2 the losses are higher than RQ is showing.

Data Breach	**$16.4M**
Ransomware	$7.8M
DDoS	$4.8M

Most Frequent

Represents the annual likelihood of occurrence based on the chosen industry and revenue size. This allows you to see how often - without taking into account your defensive posture- an attack of this magnitude could appear in your organization.

Data Breach	**1 every 3 years**
Ransomware	1 every 5 years
DDoS	1 every 10 years

Loss details based on attack type

Detailed losses for each type of attack, providing insights into both frequency and estimated financial impact.

Data Breach DDoS Ransomware

Legal $887.4K
Expenses related to legal expenses.

Remediation $1.1M
Costs associated with mitigating or resolving a security incident.

Per Record Flat Fees $2.4M
Costs associated with notification, PR, and other non-categorized losses.

Settlement $12M
Payout to the plaintiff that covers agreed costs associated with a cyber incident.

Most Frequent

Frequency, in risk assessment, indicates how often a specific event, like a cyber attack, is expected to occur within a given timeframe, aiding in risk prioritization and mitigation planning.

1 every 3 years

Estimated Loss

Represents the magnitude of financial impact you would occur to different types of cyber attacks. This number is not time bound but represents the total impact that you would face. The median value selected is where 1/2 the losses are lower than what RQ is showing and 1/2 the losses are higher than RQ is showing.

$16.4M

Peer Analytics

Explore insights by comparing your data with our curated dataset. We assess your performance against industry standards, using the maximum loss as a key metric for precise benchmarking.

Compare by Loss Compare by Revenue

Company Name	Revenue	Industry	Loss Type	Company Loss	RQ Computed Loss	Delta	Data Records	Employee Count	Attack Date
Peer 1	$31.2B	Finance and Insurance	Ransom	$15.9M	$16.4M	-$490.8K	0	6,300	09/18/2013
Peer 2	$5B	Finance and Insurance	Remediation	$16M	$16.4M	-$415.1K	3,000,000,001	14,956	08/01/2013
Peer 3	$5B	Finance and Insurance	Remediation	$16M	$16.4M	-$415.1K	3,000,000,001	14,956	08/01/2013

Disclaimer: The data displayed below shows a calculation with a pre-defined assumption with NIST CSF at level 1 and Residual Risk with controls at level 3.

Long - Term Recommendations

Long-term recommendations based on controls are strategic suggestions for maintaining and enhancing security measures and risk management practices over an extended period. These recommendations aim to ensure sustained protection and resilience against potential threats and vulnerabilities.

Improve capabilities from Level 1

1 Technical Control
Performed Informally

Control is performed inconsistently and without a standardized structure.

There are 14 evidences included

To Level 3

3 Technical Control
Well Defined

Control is standardized enterprise-wide and well-defined.

There are 36 evidences included

Annual Loss Expectancy Reduction

Annual Loss Expectancy (ALE) is a calculation that estimates the anticipated financial loss an organization might experience in a year due to recurring or one-time events, such as cyberattacks, accidents, or other adverse incidents. It is a critical metric for risk assessment and helps in planning risk mitigation strategies.

-$1.1M

Probability of Success Reduction

Probability of Success Reduction pertains to the process of diminishing the likelihood of achieving success in a given endeavor. It involves implementing strategies and actions aimed at reducing the chances of favorable outcomes. It is important to acknowledge that this simulation is based on pre-defined data, and actual results may vary depending on the inputs and real-world factors.

-18.41%

Important

The provided data is pre-defined for simulation purposes and may not reflect real-world conditions. For more accurate and enhanced results, we encourage you to consider upgrading to our RQ PRO or RQ Enterprise versions, where our dedicated Risk Engine can tailor the data and analysis to your specific needs and provide more comprehensive insights.

Learn more about us

Risk analysis results for RQ Impacts

Select a different loss level at the upper right to view the risk analysis for that loss level.

SLE Loss Types Added to CSV Export

When exporting RQ data to a CSV file, the SLE loss type and most likely value for each loss type will now be included in the file. In addition, a table summarizing the information to be exported is now provided in the **CSV Export** section of **Data Output › Data Export**.

New Permissions for RQ Fair Only User

RQ Fair Only users have the following new permissions:

- **Integrations**: RQ Fair Only users can now create, edit, use, and delete all integrations.
- **SecurityScorecard®**: RQ Fair Only users can now add SecurityScorecard domains and access the **External Data - Security Scorecard** screen.
- **Activity Log**: RQ Fair Only users can now view the activity log under **Settings › Activity Log**.

SAML

ThreatConnect RQ now supports SAML™ for single sign-on.

Integrations

ThreatConnect RQ has added the following integrations:

- **AppSoc**: This integration is an aggregator that enables ThreatConnect RQ to integrate with over 100 different security vendors and pull in vulnerability information for analysis.

Bug Fixes

- An issue causing third-party business assets with greater than 120 characters to fail was fixed.
- Currency conversions were being calculated twice. This issue has been resolved, which will lower some loss calculations for non-U.S. customers.