ThreatConnect.

BUYER'S GUIDE FOR:

Cyber Risk Quantification Solutions

Introduction

Cyber attacks have become a significant component of enterprise business risk as digital capabilities become central to business operations. However, many businesses struggle to adequately manage their growing cyber risks because they are significantly different from other risks facing the enterprise.

Why cyber risk management is important

It is well known that as enterprises, government agencies, and other organizations embrace digital transformations and evolve their digital business strategies, their attack surface grows, creating new exposures used by threat actors for more successful attacks. For example:

- Ransomware payouts increased to over $1.1 billion in 2023 [1]
- The average cost of a data breach in 2023 was $4.45 million [2]
- 61% of organizations had experienced a ransomware attack, with an average ransom cost of $1.54 million. [3]

This leads to more attacks causing a variety of direct impacts to an organization, whether that's data confidentiality and privacy, availability of business-critical assets, or affecting human safety. There is also a disconnect between what the business does and how cyber attacks are managed, measured, reported on, and mitigated.

[1] chainalysis.com/blog/ransomware-2024
[2] ibm.com/reports/data-breach
[3] assets.sophos.com/X24WTUEQ/at/h48bjq7fqnqp3n5thwxtg4q/sophos-the-state-ransomware-2023-infographic-1200-1200px_2x.png

Common Challenges with Cyber Risk Management

Visibility

- What are my risks and how do I reduce their impact?
- What risks should I prioritize?
- How do I know if I'm spending money effectively?

Effort

- It takes too long to assess cyber risks.
- There are not enough resources to assess all the risks.

Data and Analysis

- Where should I start my analysis?
- Do I have the necessary data?
- Where do I even get the data?
- How do I know if my analyses are defensible?

Quantification is the key to robust cyber risk management.

Common Use Cases For Cyber Risk Quantification (CRQ)

Putting cyber risk quantification into practice is vital to ensure the investments in a cyber risk program are realized. CRQ can support a range of use cases relevant to various teams and functions across an organization. Let's look at some of the popular CRQ use cases.

Risk & Control Mitigation Prioritization

CRQ allows cyber risk professionals and leaders to evaluate investments like their counterparts in the business, e.g., asking the question "If I have one dollar to spend, which investment is going to give me the greatest return in value?" When risks are quantified, it allows you to directly compare investments between competing opportunities.

Defining SEC Materiality / Risk Appetite

Determining the risk appetite of an organization and what is a material risk is becoming an increasingly important question to answer. The 2023 U.S. Securities and Exchange Commission (SEC) Rules on Cybersecurity requires publicly traded companies to demonstrate how they are strategically managing their cyber risks, and providing timely information to investors when a breach occurs.

Improving Cyber Risk Communication

For many CISOs, communicating cyber risk to business leaders, executives, and directors is a constant challenge. CRQ helps to break down barriers between the parties by enabling the CISO to have risk conversations in the language business-leaders understand - money.

Vulnerability Prioritization

CRQ provides the potential financial impact to business assets, allowing the vulnerability management team to know which assets are truly business-critical (i.e., they have the highest financial impact to the business). This allows them to invest in remediating vulnerabilities that will generate the greatest risk mitigation return on investment.

Third Party & Supply Chain Risks

Cyber risk quantification enables risk managers to know which business assets (and processes) are most critical to the organization. It provides organizations with a standardized approach to assess and compare the security posture of different suppliers. CRQ allows risk managers to effectively communicate with leaders and executives in business terms, improving collaboration and risk decision making.

Compliance with Regulations & Frameworks

CRQ helps organizations demonstrate compliance with regulations and frameworks. It makes allocating investments in security controls demonstrable and defensible, and be able to demonstrate the alignment with an organizations' cybersecurity strategy.

Communicating That an End of Life (EOL) System Should Be Retired

Many companies use CRQ to show that the financial risk of the older system is much greater than the newer system, and that by leaving the older system online, the financial risk to the business is large. CRQ helps enable the business to make the decision to retire the system due to the financial burden, not technical risk metrics.

Exception or Gap Management

Companies using CRQ can calculate the financial risk of exceptions to IT system and application changes (patches, configuration changes) before they are granted and allow security to say "yes you can have the waiver from security if you accept this financial risk".

CRQ Solutions

Tools and Technologies are needed to bridge the people doing and responsible for cyber risk and processes that drive the program. The current tools used to do risk quantification include:

Spreadsheets

A very common option. Simple to implement, but expensive to maintain and they don't have the ability to scale along side a CRQ program.

Custom-built, proprietary applications

Another popular option for organizations with large budgets and access to experts in threat modeling, risk quantification, data science, and AI engineering.

Purpose-built, commercial solutions

This is the traditional route for many organizations once they graduate out of using spreadsheets. There are a variety of apps on the market, with most focused on enabling FAIR assessments, and modern apps that take a post-FAIR approach.

The current state of CRQ solutions is primarily centered around in-house, purpose-built applications or customized spreadsheets, and commercially available software and platforms focused on implementing the FAIR approach.

- In-house applications and the use of customized spreadsheets exist where organizations had very early efforts to quantify risk, before commercial solutions existed, or were in the purview of businesses with existing expertise in both cybersecurity and business-risk quantification. Most organizations putting CRQ into practice tend to leverage spreadsheets because they are familiar and offer a good starting point for doing basic risk analytics. Yet, they are limiting for the usual reasons - they're general purpose analysis tools that are not optimized for dealing with large, diverse data sets and performing advanced analytics, like machine learning. And like other customer business applications, they also require considerable internal investments to maintain and can be impacted with the loss of subject matter experts.
- Commercially available FAIR-based software solutions emerged alongside adoption of the FAIR approach. These tools make doing FAIR-based analysis easier as they are purpose built to facilitate this specific approach to doing cyber risk quantification. However, as FAIR is an involved methodology to quantitative assessing risks, these tools still require risk managers to collect, process, and maintain their own data sets, and the approach is highly-subjective, such that these tools do not apply other risk quantification models, like ones that leverage AI and machine learning.

However, a third commercial option has emerged in the last few years – data and AI-powered CRQ platforms.

- The cutting-edge approach to putting CRQ into practice is being addressed by data and AI-powered SaaS solutions. These platforms were constructed to address the limitations of trying to build and maintain in-house solutions, and the required learning-curves and limitations of FAIR-based solutions. These modern solutions solve the challenges with having the necessary data and fit-for-purpose analytical models to perform analyses, and making it easier to perform risk quantification without needing a high-degree of subject matter expertise.

Comparison of Platforms

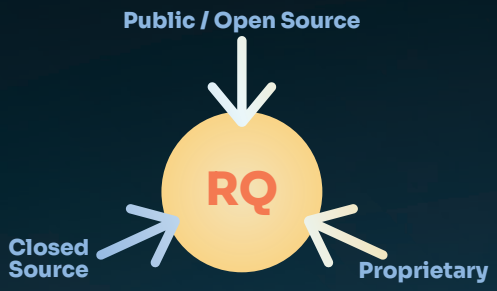
The table (below) summarizes the key attributes CRQ buyers need to consider when purchasing a solution, and how well the three technical approaches to operationalizing CRQ address the attributes.

Key Attributes	Solution Type		
	Built In-House / Spreadsheets	FAIR-Based Solutions	Data and AI-Powered SaaS Solutions
Provides robust industry-wide data	○	○	●
AI and ML-powered analytics	○	○	●
Scales to thousands entities/business and assets	○	◑	●
Automated analysis	○	○	●
Supports a range of analytic methods	◑	○	●
Customizable analytics	●	◑	●
Enterprise-wide down to business-level views	◑	◑	●
Peer comparisons	○	○	●
Use of industry standards and frameworks (i.e., ATT&CK)	○	○	●
Supports a wide-range of use cases	◑	◑	●

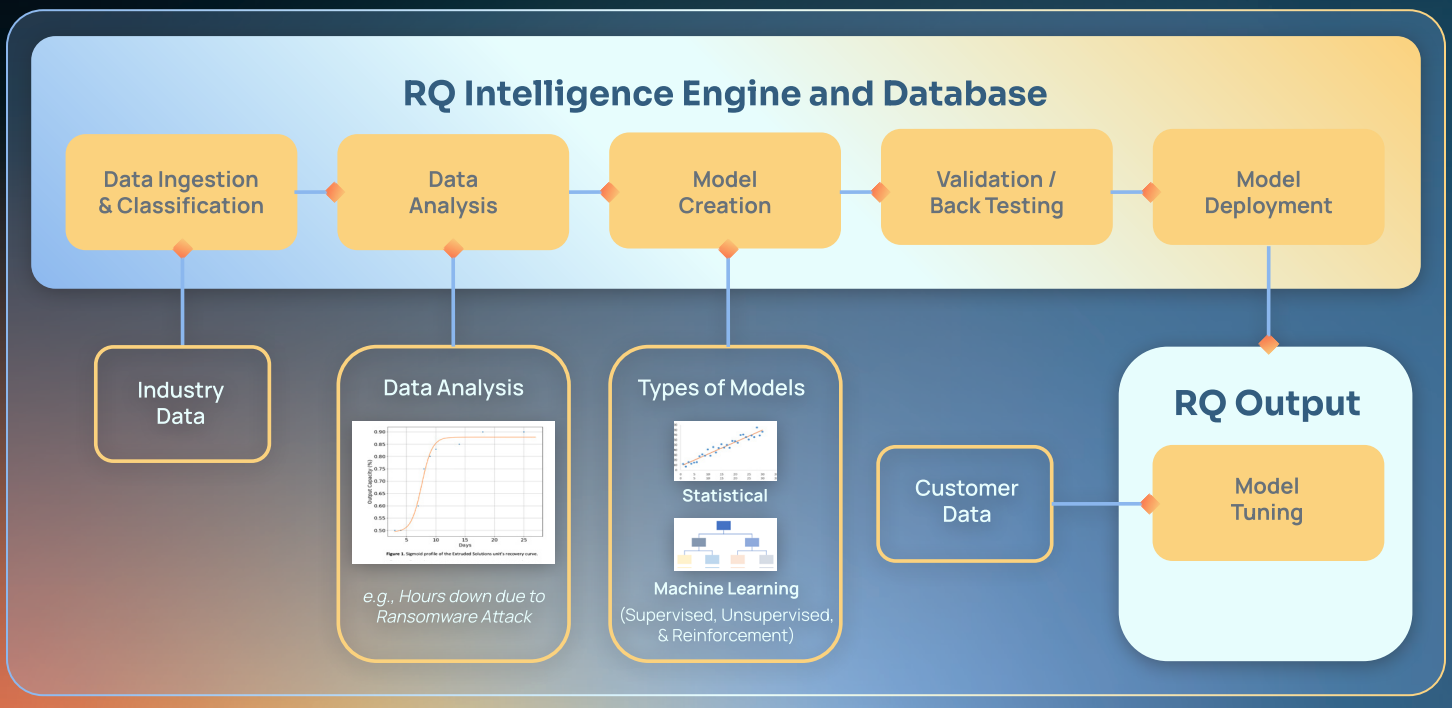
Introducing ThreatConnect Risk Quantifier

ThreatConnect Risk Quantifier (RQ) is the market-leading, modern data and AI-powered solution to help you operationalize cyber risk quantification. ThreatConnect RQ solves the technical challenges discussed in this guide in the following ways:

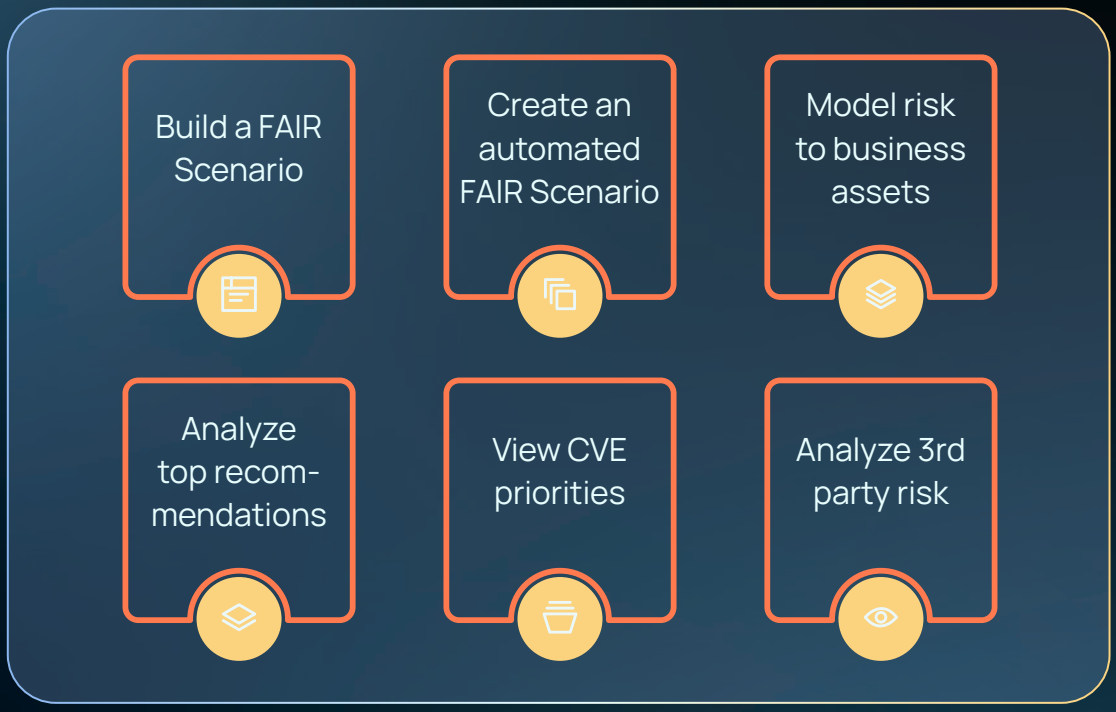
- Removes the need for collecting, processing, and maintaining the data required to produce robust cyber risk analysis outputs. RQ does all the data collection and management heavy lifting so you don't have to worry about it.



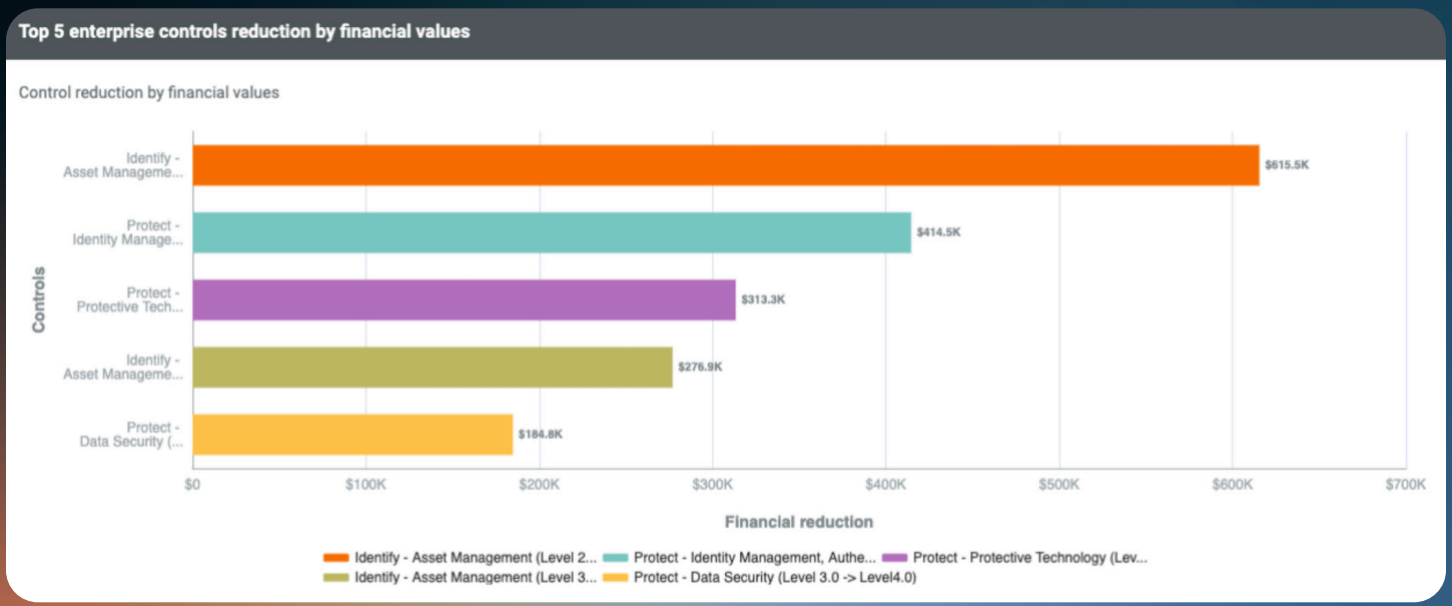
- Provides AI and ML-powered analytics that have been tested and vetted to make cyber risk analysis faster and easier, without needing to be a deep subject matter expert in data analytics and cyber risk.



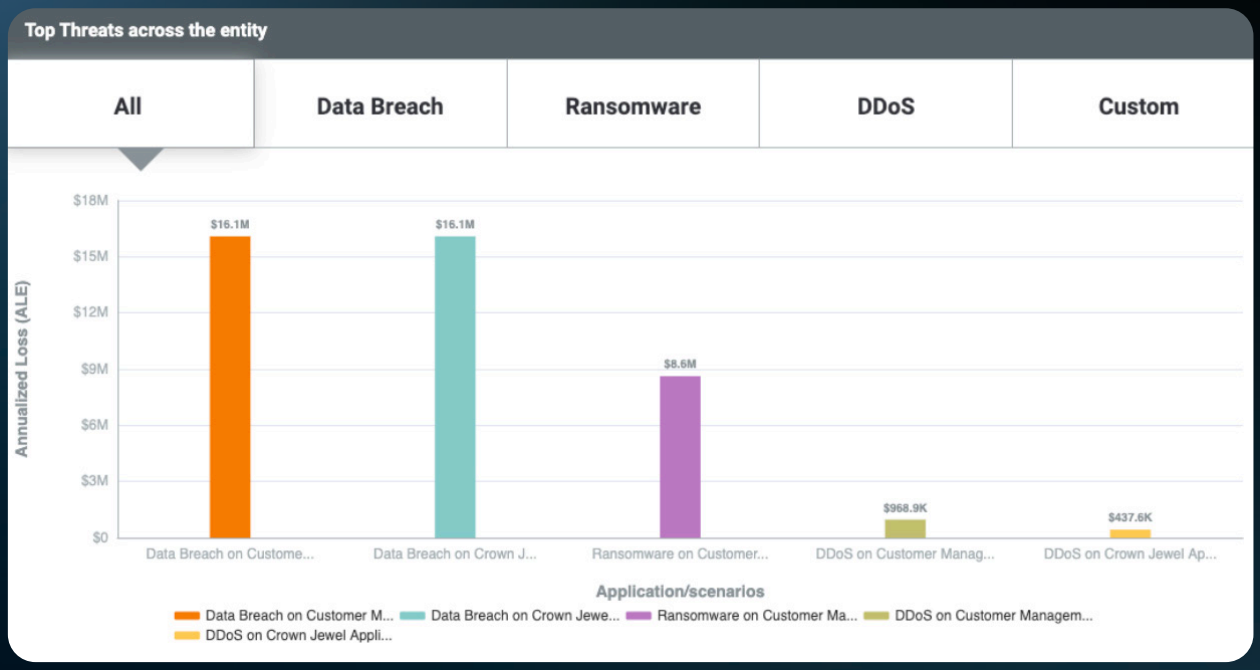
- Extensible to your preferred approach to quantifying cyber risk, whether using FAIR, Semi-FAIR, our proprietary models, or custom models, allowing you to evolve your current CRQ approaches over time.



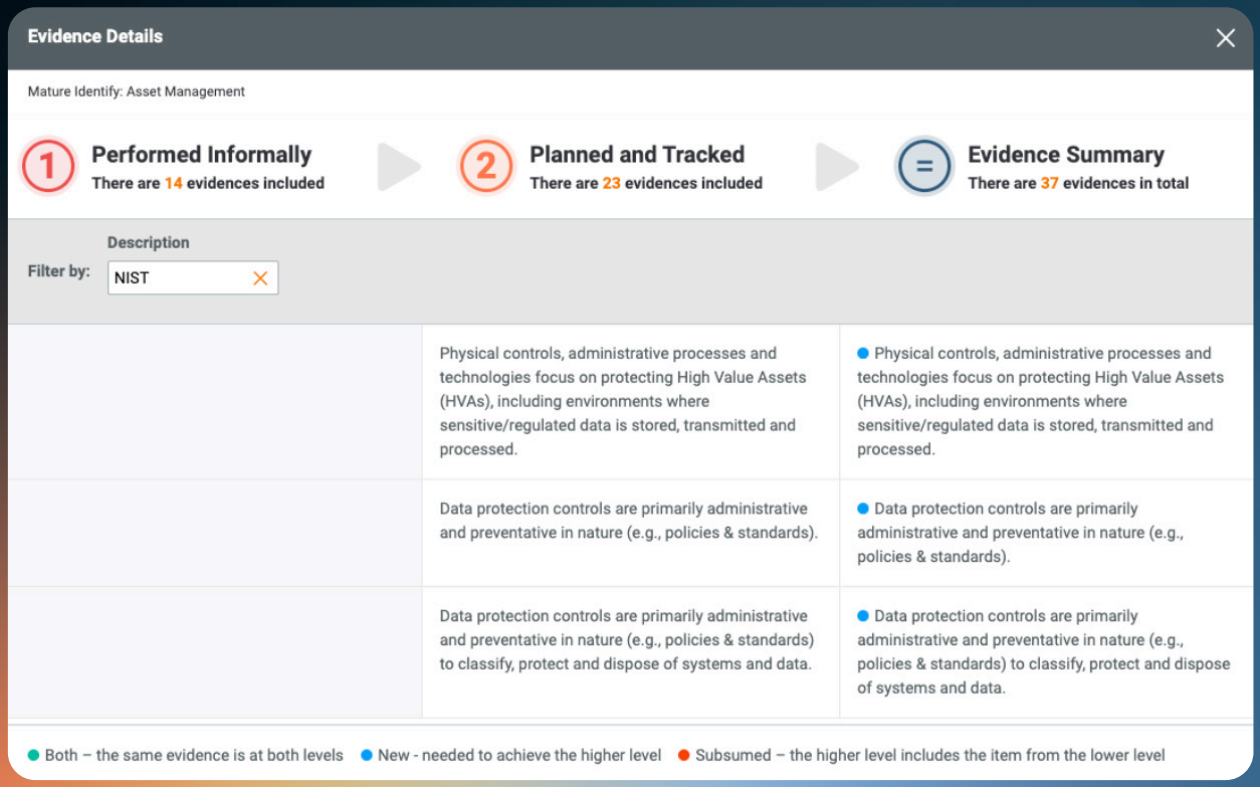
- Leverages industry standards and frameworks, such as ISO27002, MITRE ATT&CK, and others as part of the security controls.



- Provides defensible financial impact outputs, enabling you to have effective cyber risk conversations with application and business owners, executives, and directors, leading to improved decision making on risk management and mitigation.



- Makes compliance with industry frameworks and regulatory requirements easier, such as knowing what constitutes a material impact for the SEC Cybersecurity Rules in the U.S., and to always be audit-ready when addressing internal, external, and third-party audits.



Learn how ThreatConnect RQ can modernize your cyber risk quantification program

Thanks for taking the time to learn about how to put cyber risk quantification to work in your organization. If you'd like to learn more about cyber risk quantification or ThreatConnect's RQ solution, please visit threatconnect.com/RQ or reach out to us at threatconnect.com/request-a-demo.

ThreatConnect.

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. Over 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets.