Risk360

Quantifying Cyber Risk in Financial Terms for Strategic Decision-Making

WHITEPAPER

Background

Cyber breaches are growing in both frequency and their potentials for significant financial impact. Organizations are increasingly recognizing the need to quantify cybersecurity risks in financial terms to make informed, strategic decisions.

Translating cybersecurity risks into financial terms empowers executive leadership to:

- **Define Acceptable Risk:** Understand and set organizational risk tolerance levels.
- **Optimize Risk Transfer:** Inform decisions on cyber insurance coverage and allocation.
- **Prioritize Investments:** Justify technology investments and resource allocation for maximum mitigation impact.

Traditionally, quantifying cybersecurity risks in financial terms has been difficult for several reasons:

- **Intangible Risks:** The inherent complexity of cyber threats makes them difficult to score and measure, hindering accurate financial loss quantification.
- **Dynamic Threat Landscape:** The ever-evolving nature of cyber threats complicates accurate prediction of potential financial impacts.
- **Lack of Standardized Metrics:** The absence of universally accepted metrics has led to inconsistent and subjective risk assessments.

Benefits of Financial Risk Analysis with Risk360

At Zscaler, we developed Risk360 to provide a holistic view of your organization's cyber risk. Its integrated Financial Risk module goes a step further translating these risks into quantifiable financial terms. It provides the following capabilities:

1. **Yearly Average Loss:** Risk360 provides a clear estimate of your organization's annual financial exposure, accounting for your current cyber risk posture and the protective controls gained through Zscaler solutions. Crucially, it also forecasts the potential reduction in Yearly Average Loss if you remediate your top ten risk factors, highlighting clear pathways for improvement (see Figure 1).

2. **Loss Curve Analysis:** Visualize your Yearly Average Loss over time through a historical trend line, enabling you to track progress in reducing financial exposure (see Loss Curve section in Figure 1).

3. **Financial Exposure of Top Ten Factors:** To facilitate targeted remediation and demonstrate clear ROI, Risk360 details the specific financial exposure associated with each of your top ten risk factors (see Top 10 Financial Contributing Factors in Figure 1).

4. **Comparison of Yearly Average Losses:** Gain critical insights by comparing Yearly Average Losses across four distinct scenarios (See Average Yearly Exposure section of Figure 2). The four scenarios are as follows:
   a. **Inherent Risk:** Represents a scenario based on the current risk score
   b. **Last 30 Days Average Risk:** Represents a scenario based on the average risk score in the last 30 days
   c. **Residual Risk:** Your projected risk after mitigating the top ten identified risk factors
   d. **Industry Peer Risk:** Represents a scenario based on the average industry peer risk score

5. **Breach Probability:** The breach probability has a value between zero to one and is an input parameter for the financial exposure. The value of Zscaler–calculated breach probability is continuously updated and determined based on the industry vertical, annual revenue range and the organization risk score. Risk360 shows the breach probability based on Inherent Risk, Last 30 Days Average Risk, Residual Risk and Industry Peer Risk scenarios (See Breach Probability section of Figure 2).

6. **Loss Exceedance Curve:** Understanding that cyber breaches and their financial impacts are probabilistic, the Loss Exceedance Curve shows the probability of financial losses exceeding various thresholds. This crucial insight directly supports strategic decisions regarding cyber insurance coverage and acceptable risk transfer (see Loss Exceedance in Figure 2).

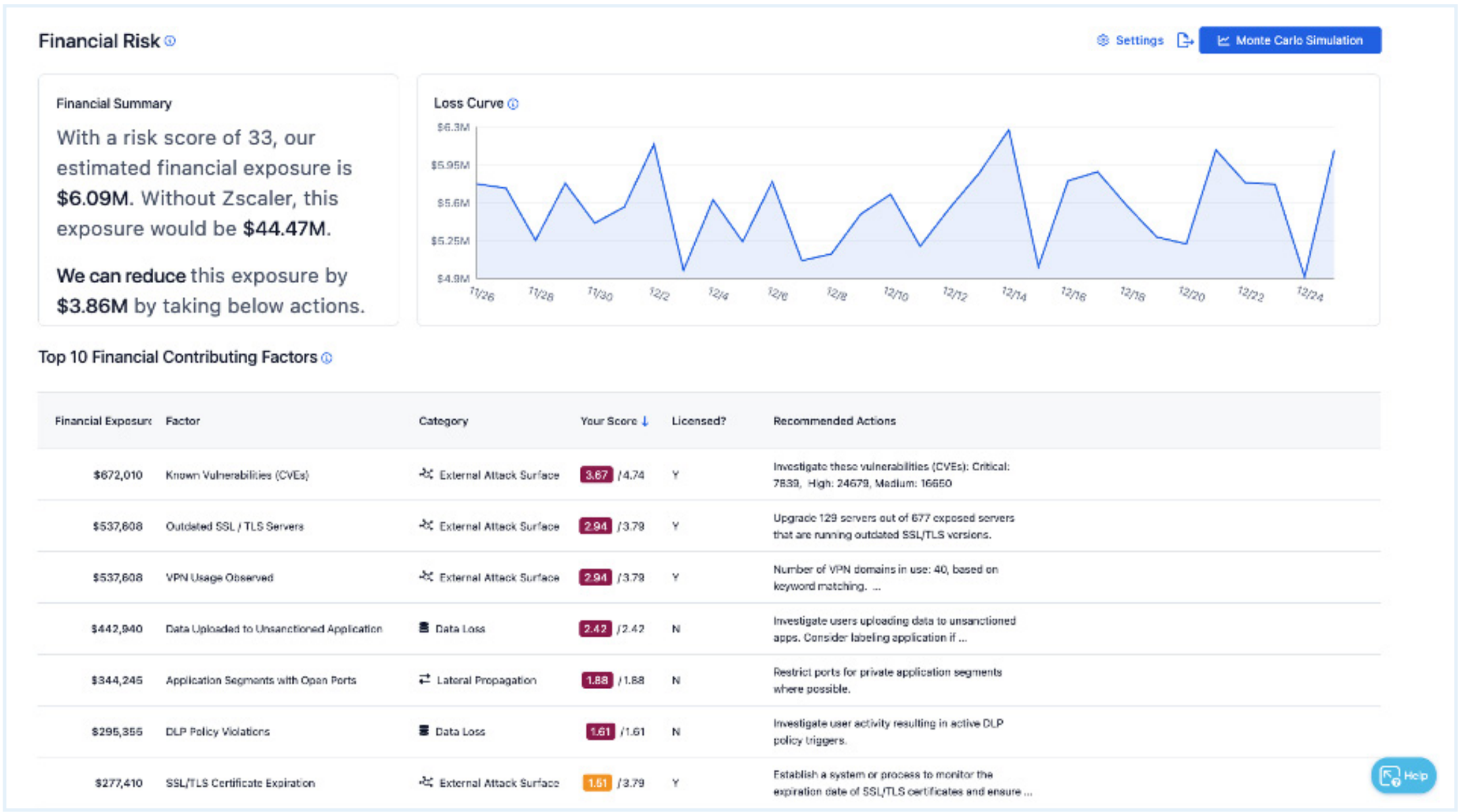

Figure 1: Overview of Financial Risk

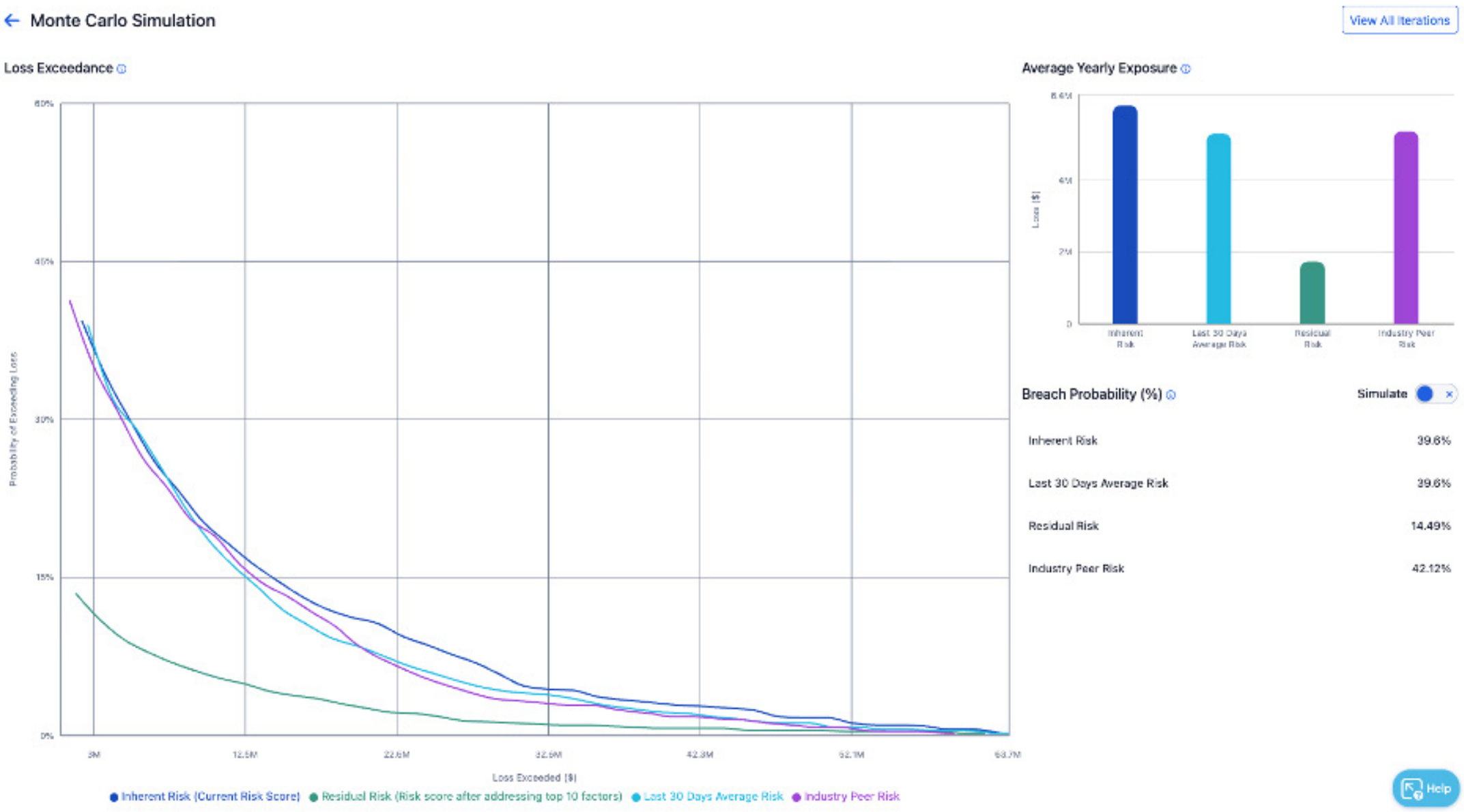

Figure 2: Monte Carlo Simulation

Methodology

Our methodology of quantifying cybersecurity risks in financial terms is built on robust data. We begin by collecting extensive information on historical cyber breaches from organizations not leveraging Zscaler solutions.

We use this information to estimate the probability of a cyber breach for organizations within a specific industry verticals and annual revenue category which is not using Zscaler solutions (refer to Appendix for details). We then tailor and adjust this probability for your organization based on your real-time Risk360 risk score, reflecting the specific efficacy of your Zscaler-protected environment..

Similarly, we analyze reported financial losses to define a lower/upper bound (confidence interval) for the financial loss when an organization in a given industry vertical and a particular annual revenue size experiences a cyber breach.

Risk360 also offers the flexibility for customers to customize key input parameters, ensuring the financial model accurately reflects the unique realities and specifics of their organization (See Figure 3).

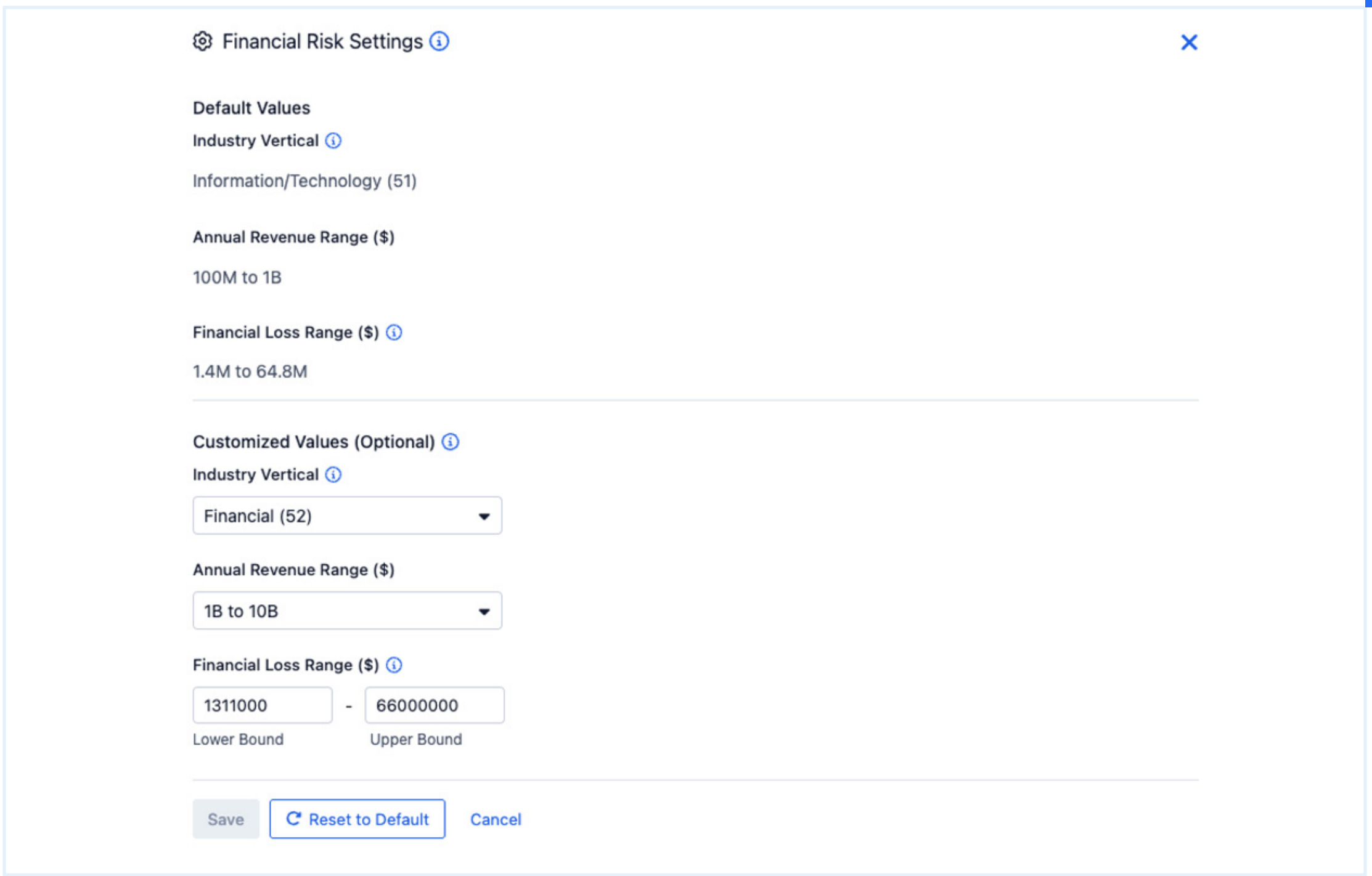

Figure 3: Customizing the Financial Risk Settings

The core of our financial risk quantification follows the widely accepted formula:

Financial Risk = Likelihood (Probability of a breach) **x Impact** (The severity of the consequences when a breach happens)

The Impact, i.e. the severity of the consequences when a breach happens is probabilistic and we have defined a log-normal continuous probability distribution to estimate the impact of a breach when a cyber breach occurs.

We then run Monte Carlo simulations, one thousand times. Monte Carlo simulations is a computational technique that uses random sampling to analyze the impact of uncertainty in a system. When we run the Monte Carlo simulations, the Likelihood i.e. the probability of a breach determines the simulation results that represent an actual breach. The Impact for the simulation results that represent a breach is determined through a randomized financial loss within the defined confidence interval. We average the results of simulations (see Figure 4) to produce the Yearly Average Loss and use the same simulation results to produce the Loss Exceedance (see Figure 2).

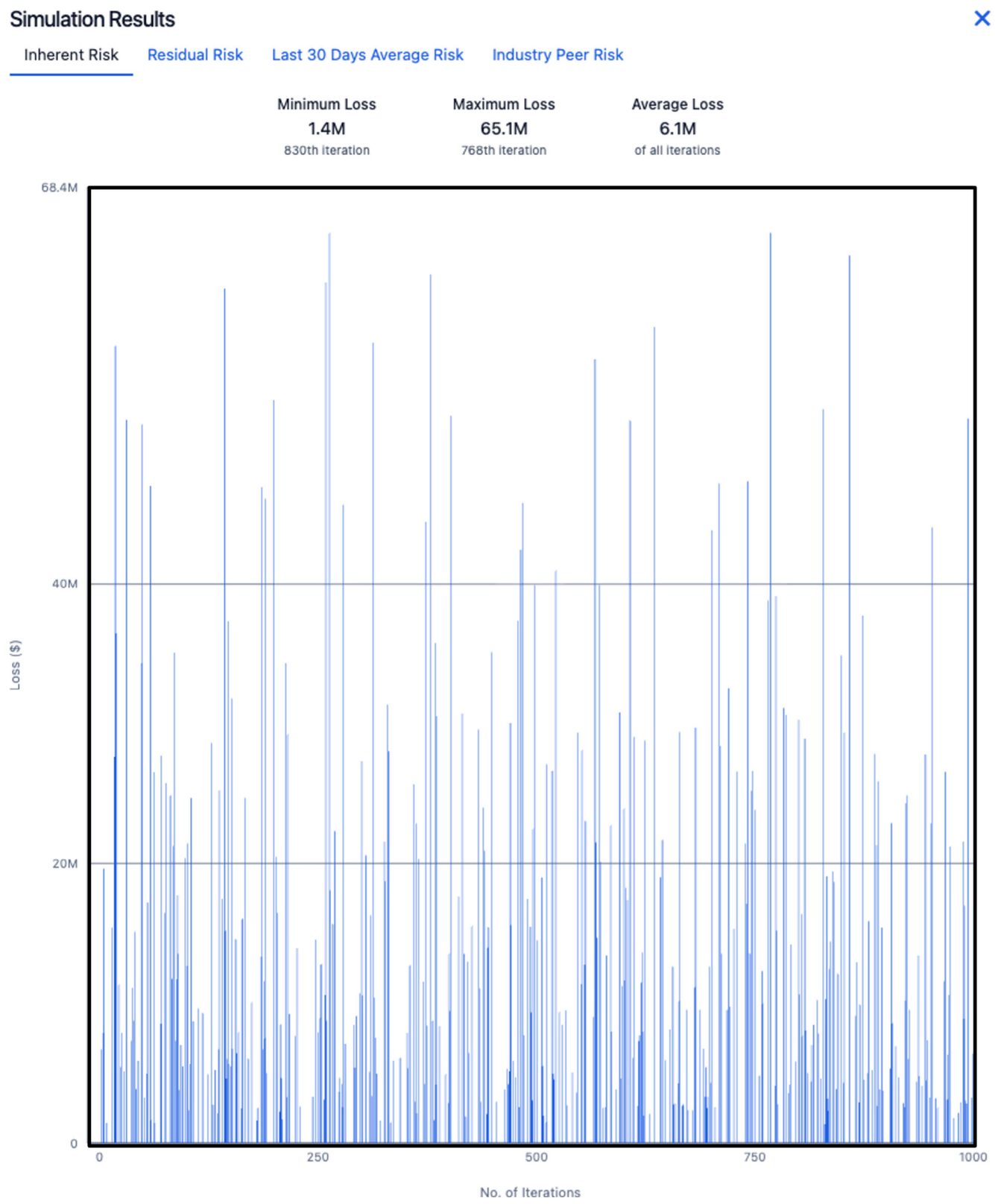

Figure 4

Empowering “What-if”Scenario Planning

A critical feature for strategic planning, the Financial Risk module of Risk360 enables robust “what-if” analyses. This allows you to model the financial impact of various breach probability scenarios.

As explained in the previous section, the breach probability is an input parameter for your organization’s financial exposure calculation. The value of Zscaler-computed breach probability is continuously updated and determined based on the industry vertical, annual revenue range, and the organization’s risk score.

You can actively manipulate this probability using the ‘Simulate’ toggle, adjusting it for specific scenarios. Upon applying changes, Risk360 instantly re-evaluates your financial exposure, providing immediate feedback. Disabling the toggle seamlessly restores the Zscaler-computed probabilities.

Figure 5

Conclusion

Integrating sophisticated financial modeling into cybersecurity risk management represents a profound advancement in how organizations strategically approach and understand cyber threats. By providing a clear, quantifiable and actionable measure of cybersecurity risks in financial terms, Zscaler Risk360 empowers your leadership team to navigate the complex cyber landscape with unparalleled confidence, precision, and strategic advantage.

Appendix

INDUSTRY		
Administrative	Information	Real Estate
Education	Management	Retail
Entertainment	Manufacturing	Trade
Financial	Other	Transportation
Healthcare	Professional	Utilities
Hospitality	Public	

REVENUE CATEGORY
$10M to $100M
$100M to $1B
$1B to $10B
$10B to $100B
More than $100B

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Act Fast.
Stay Secure.