



# How do you **Measure & Mitigate** cyber risk?

---

White Paper

# Executive Summary

## Increasing Cyber Threats

As businesses continue to invest in digital transformation and base their business model on technology, cyber threats only become more imminent. Cyber attacks are growing more sophisticated, occurring once every 39 seconds, the IBM Cost of Data Breach Report, 2020 reports an average cost of data breach to be \$3.86 million annually. In such a volatile environment, a robust cyber security plan becomes imperative. It aids organisations to make better decisions, improve their cyber security risk posture, mitigate the consequences of cyber crime, gain more visibility into their threat landscape and finally, improve their cyber resilience.

## Business Impact of Cyber Threats

Cyber Risk is now a board-room concern. With cyberattacks disrupting business continuity, they pose a direct impact on the top and bottom line of an organization's balance sheet. Thus, making cybersecurity as one of the top priorities of every organization

According to Forbes, lack of Cyber Resilience is the top global business risk in 2020. In 2019 alone, an estimated 8.5 billion accounts were compromised. The CISO Benchmark Report 2020 states that the most impacted business areas after a security breach are operations and brand reputation; followed by finances, intellectual property, and customer retention.

## What are the challenges with traditional cybersecurity approach?

The evolving breach trends verify that complying to frameworks alone can no longer holistically safeguard organizations. Frameworks such as ISO, NIST, PCI DSS and others are used as reference checklists for cybersecurity and risk management practices, however, provide limited visibility. Cybersecurity must be aligned with every organization's threats and mission-critical business needs, provided by products that deliver holistic and actionable insights. The Frameworks approach to risk-posture assessments are subjective, labor-intensive, and only offer point-in-time snapshots/assessments. They rely on a qualitative scale without any objective and quantitative measure to assess the security posture of an organization.

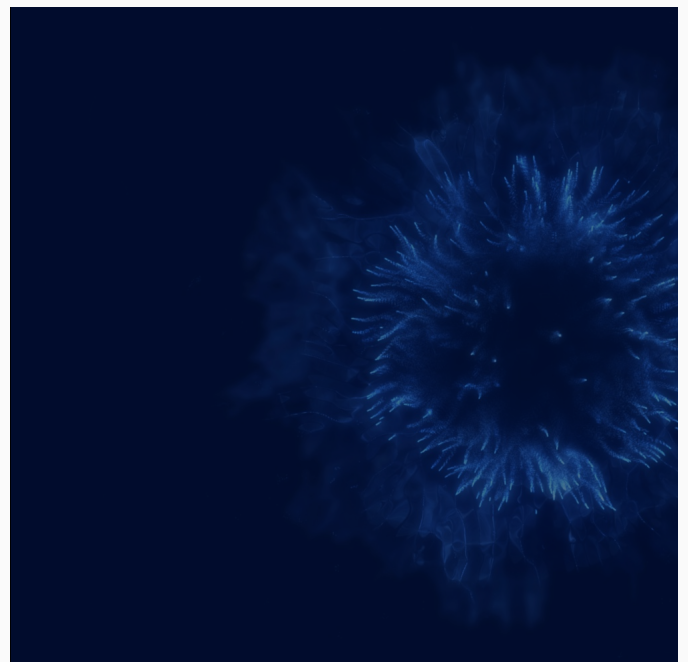
Similarly, Security Rating Services represent an independent source of publicly accessible data to support some use cases. However, these services don't provide a complete assessment of security controls, as their information is primarily sourced from publicly accessing internet IP addresses, honeypots, analyzing Deep and Dark web content, and individual proprietary data warehouses.

# The new approach of looking at cybersecurity!

## Cyber Risk is everyone's responsibility

Today, the delegation of risk decisions to the IT team cannot be the only solution and has to be a shared responsibility. The board and business executives are expected to incorporate the management of cyber risk as part of their business strategy since they are accountable to stakeholders, regulators and customers. For the CROs, CISOs, and Security and Risk Management Professionals to be on the same page, there has to be a single source of truth for communicating the impact that cyber risk has on business outcomes, in a language that everyone can understand.

This is where Cyber Risk Quantification comes in as a game-changer. There is a need for a solution which integrates with the entire security stack and gives a measurable analysis that supplements decision making. This comprehensive information empowers CISOs and executives to make informed and timely decisions to ensure the cybersecurity of the



## Continuous Assessment of Cyber Security is the need of the hour

Compliance and government guidelines mandate the move to go beyond periodic assessments and into continuous monitoring of sensitive and critical information. In such situations, a CISO may often be unable to quantify the maturity of the Information Security measures deployed in the organization. Continuous Assessment of Cyber Security lets an organization prioritize the key focus areas across their Critical Assets and most vulnerable technology verticals. This ensures that adequate measures towards holistic Cyber Security maturity are adopted throughout the organization.

## Objectivity and simplicity should be at the core of your cybersecurity strategy

Cybersecurity posture cannot be represented by lengthy reports only. It needs to become objective and help decision makers truly understand the risk posture and the dollar value risk that the organization faces. It also needs to be free from IT jargon to enable the boardroom to have a clearer view of the risk posture, thereby facilitating data driven and informed decisions. Executives can get overwhelmed with excruciating details from multiple tools or people. They can now rely on all the data that has been collected and converted from these sources into a simple yet comprehensive score that they can use to track and build their trust on.

# SAFE Approach

The Security Assessment Framework for Enterprises (SAFE) attributes an enterprise-wise, unified, objective and real time score which empowers organizations to understand and improve their cyber risk posture. Designed from the ground up with simplicity, standardization and compliance guidelines in mind, SAFE provides a quantitative dimension to cyber risk management. The SAFE score ranges from 0.00 to 5.00 and rates the breach likelihood of an organisation at both macro (enterprise/ location) and micro (individual IP/ asset) levels.

## Our 5 vector approach



### People

A zero-permission mobile application that helps users protect their phones against hacking by monitoring its cybersecurity controls. It also allows the enterprise to run cybersecurity awareness campaigns from a library of over 100 nano cybersecurity training videos and quiz along with monitoring if the employee's personal information/passwords are leaked in the deep and dark web. This data is then put together in our Scoring Engine to give a score per employee

### Policy

Policies wrap around the entire digital infrastructure to safeguard the security hygiene encompassing all functions in an organisation. With over ten years of experience, we have formulated a vast repository of over 40 policies broken into 4500 controls which are derived from globally accepted compliances like ISO, NIST, HIPAA, PCI DSS and others, that could be applied to your enterprise.

## Technology

SAFE covers your entire technology stack- its applications, cloud services, databases, Network and security nodes, end points and a lot more. It assesses the cyber security posture of each asset based on CIS benchmarks for configuration, NVD for vulnerabilities and threat intelligence from internal and external sources. This gives a true picture of how secure your internal technology set-up is.

## Cyber Security Products (CSP)

There is potentially a cyber security product for every niche requirement. Investing in, using, collecting and analysing the 'relevant' information becomes a mammoth task for the security team. SAFE provides guidance into procuring must-have and good-to-have products based on your organization's geography, industry and size. Based on the usage, SAFE provides a score to solve your cyber security problem. SAFE acts as a unified dashboard that sifts through the already existing data and gives you a real-time holistic view with prioritised actionables.

## External

53% of organizations have experienced one or more data breaches caused by a third party. SAFE can automatically assess all the organisation's third parties and provide a cyber risk posture assessment. SAFE can also scan the deep and dark web to provide visibility into leaked credentials for the first and third party.

## SAFE Use Cases



Understanding cybersecurity posture of an



Ensure Compliance with industry-recognized standard



Deep and Dark Web Monitoring



Measure and improve Cybersecurity awareness of your employees.



Configuration assessment and Vulnerability Management of the technology stack.



Visibility and configuration assessment of cyber security products.




Outside-in assessment of third-parties


# How does SAFE measure cyber risk?

SAFE scores and provides actionable insights as an outcome






Reputation Risk



Regulatory Risk



Financial Risk

- Overall SAFE Score for the Enterprise clubbed to \$ Value Risk
- SAFE Score for Business Units
- SAFE Score for Internal Technologies (per IP/Applications)
- SAFE Score for External Technologies
- SAFE Score for Policies / Processes
- SAFE Score for Employees
- SAFE Score for Third Parties
- SAFE Score for Compliance Management
- SAFE Score for Custom Asset Groups

## SAFE Scoring Model

“Likelihood of Breach” for an enterprise is a direct function of gaps in People, Process, and Technology. The SAFE score is, therefore, a function of “Likelihood of Breach” both at a macro (organization level) and at micro-level (per employee, policy, and asset). Suggestions from subject matter experts (SME) are taken into consideration while selecting inputs for the scoring model and information which satisfy the following criteria :

### Clear

Everybody/anybody knows what that means.

### Observable

The decomposed object should be observable and one should be clear, what would happen when we observe more of that object/vulnerability.

### Useful

Taking into consideration only those things that really matter in decision making.

In the SAFE Scoring model, the Scores are provided at the following levels



**External Third-Party**

SAFE Score with confidence metric for the third party considering the assessment of only external controls.

## Expected Loss

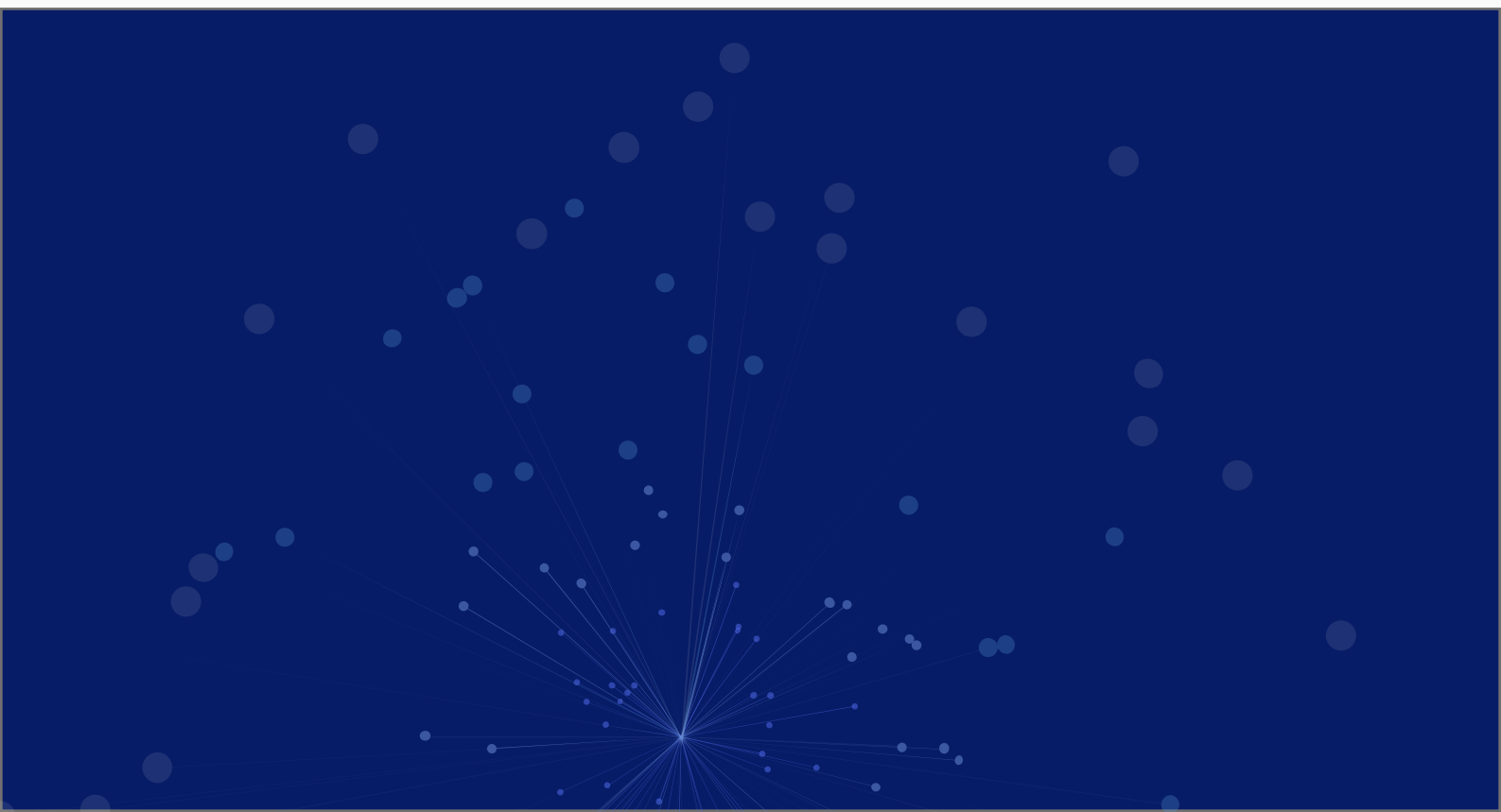
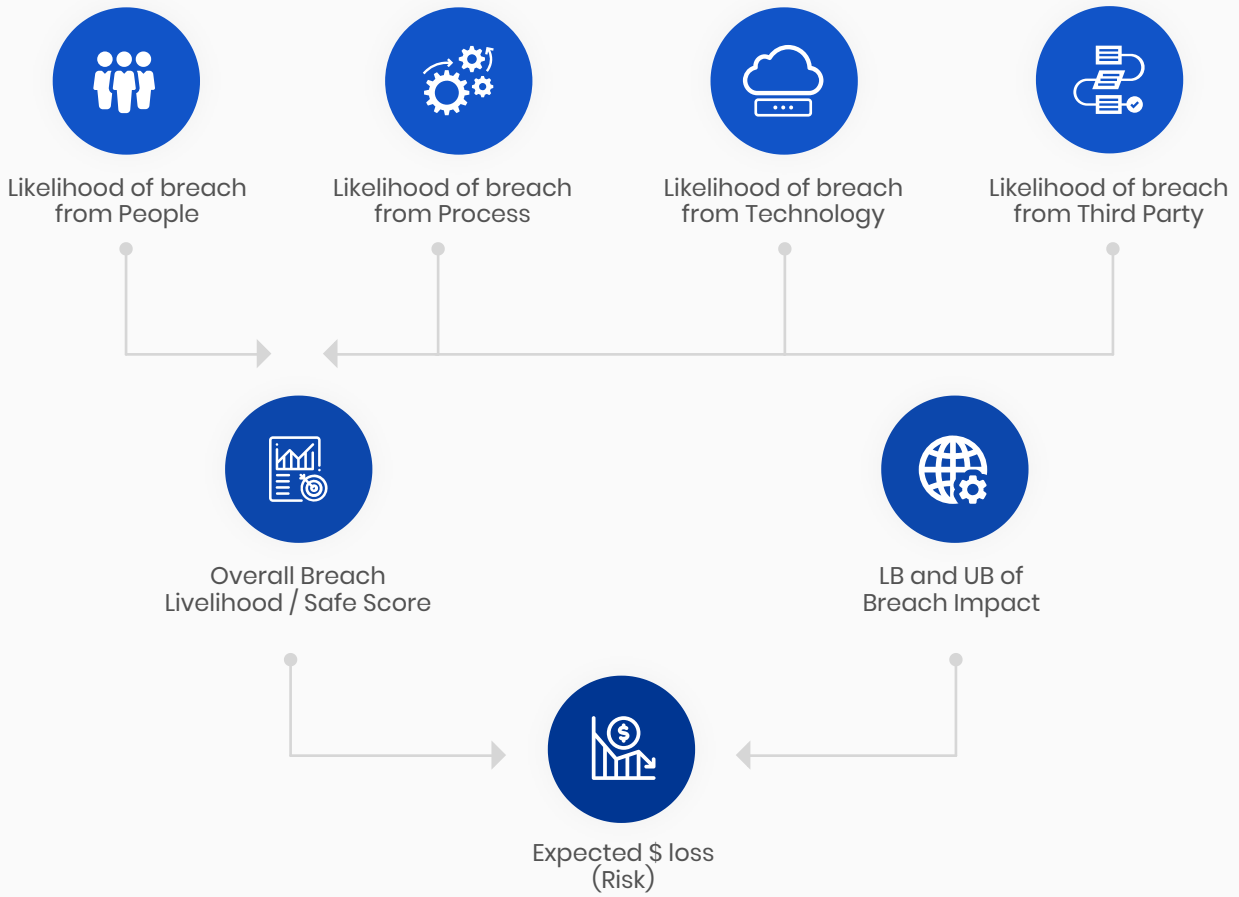
The overall risk (expected loss) faced by an organization is a direct function of Breach Likelihood & Breach Impact (based on extensive study of average breach cost). The overall likelihood of a breach is used as an input in Poisson distribution to calculate the Breach Frequency Distribution. Poisson distribution is popularly used in:

Insurance sector to estimate the claims count.

- Insurance sector to estimate the claims count
- E-Commerce Industry to estimate number sales in a given time period



The Breach frequency distribution and breach impact inputs are then combined using Monte-Carlo simulation to get the expected loss or the Risk the company is facing.





# SAFE Benefits & Key Highlights



SAFE brings the entire cybersecurity assessment to one platform, improving work efficiency by eliminating the need to monitor multiple applications & platforms.



SAFE is proactive and alerts organizations in real-time towards security gaps with 100% IT infrastructure coverage.



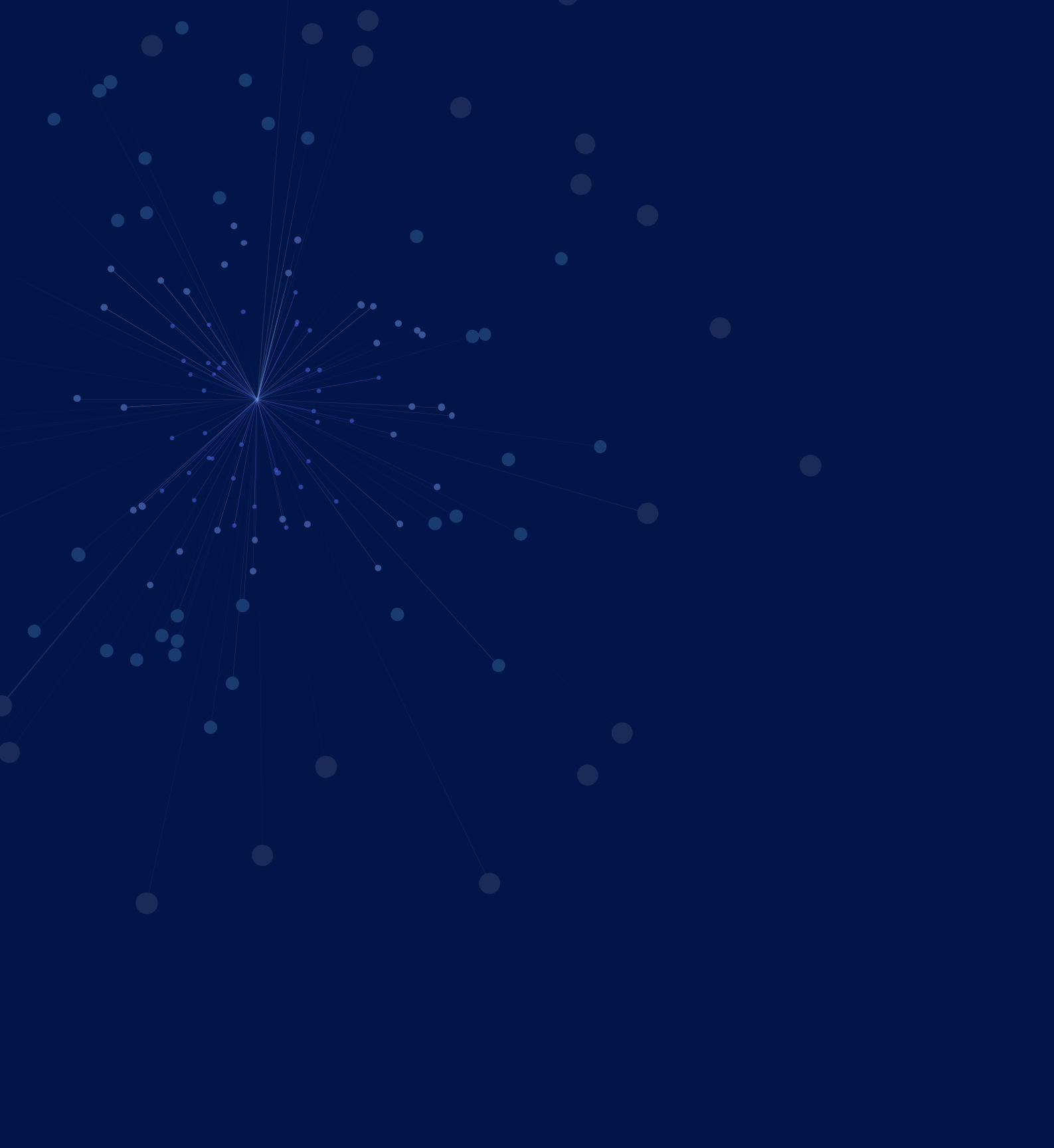
SAFE provides an estimate for improving the cybersecurity posture of an organization by keeping the current security posture as a benchmark and defining the roadmap whilst prioritizing key areas of concern.



Measure, Monitor and Mitigate Risks per LoB (Business Unit) / Crown Jewels.



Enables the Board, CISO & Security Analysts to be aligned with an objective risk metric that takes into account both, technical & the business context and gives prioritized actionables.



[www.safe.security](http://www.safe.security) | [info@safe.security](mailto:info@safe.security)

Stanford Research Park,  
3260 Hillview Avenue,  
Palo Alto, CA - 94304

