FACT SHEET

Return On Security Investment Module

SAFE

Get the maximum return on your cybersecurity investments with SAFE's ROSI calculator

The Return on Security Investment (ROSI) for every budget decision is under scrutiny. Security and Risk Management leaders face increasing pressure to prove the value and impact of their investments and have tough questions to answer:

- ***Are we investing in the right cybersecurity initiatives?***
- ***What is the business impact of a cybersecurity investment?***
- ***Are we maximizing our business risk reduction through our cybersecurity budget?***
- ***Does our cyber insurance adequately meet our needs?***

Risk leaders have relied on commercially available ROSI calculators that present significant challenges: **they're manual, point-in-time, and make subjective assumptions.**

Until now, there has been no baseline that can give you **the confidence you need to make defensible decisions**.

Quantifying cyber risk and understanding the return on your security investment in real-time enables you to identify and prioritize the initiatives that will **generate the maximum return.**

Delivering Value Across Your Organization

For CEOs, CFOs, Board Members

- Understand the financial impact of cybersecurity risk on business revenue and growth
- Evaluate your cyber risk management plan objectively – without assumptions

For CISOs, CIOs

- Understand the return on investment across security initiatives: defense, mitigation, response, recovery, and insurance
- Confidently communicate your real-time cyber risk posture to stakeholders
- Integrate cybersecurity risk with operational risk management to ensure business continuity

For Risk and Insurance Practitioners

- Get a dollar-value metric to measure cybersecurity risk
- Connect cybersecurity strategies to overall risk reduction and understand the risk being underwritten or transferred

Calculate your ROSI in Real-Time - Now Available in SAFE

Prioritize security investments based on the potential risk to your business
Add, adjust, or remove initiatives according to your acceptable levels of financial risk.

Identify the initiatives that will have the greatest return on investment
Confidently invest in the most impactful initiatives and make every dollar count.

Integrate cybersecurity risk management into your enterprise risk
Elevate cybersecurity risk as an operational risk to protect your revenue and growth.

Negotiate a fair cyber insurance premium for your business with real-time insights
Learn what percentage of your cyber risk can be transferred with the largest impact

SAFE

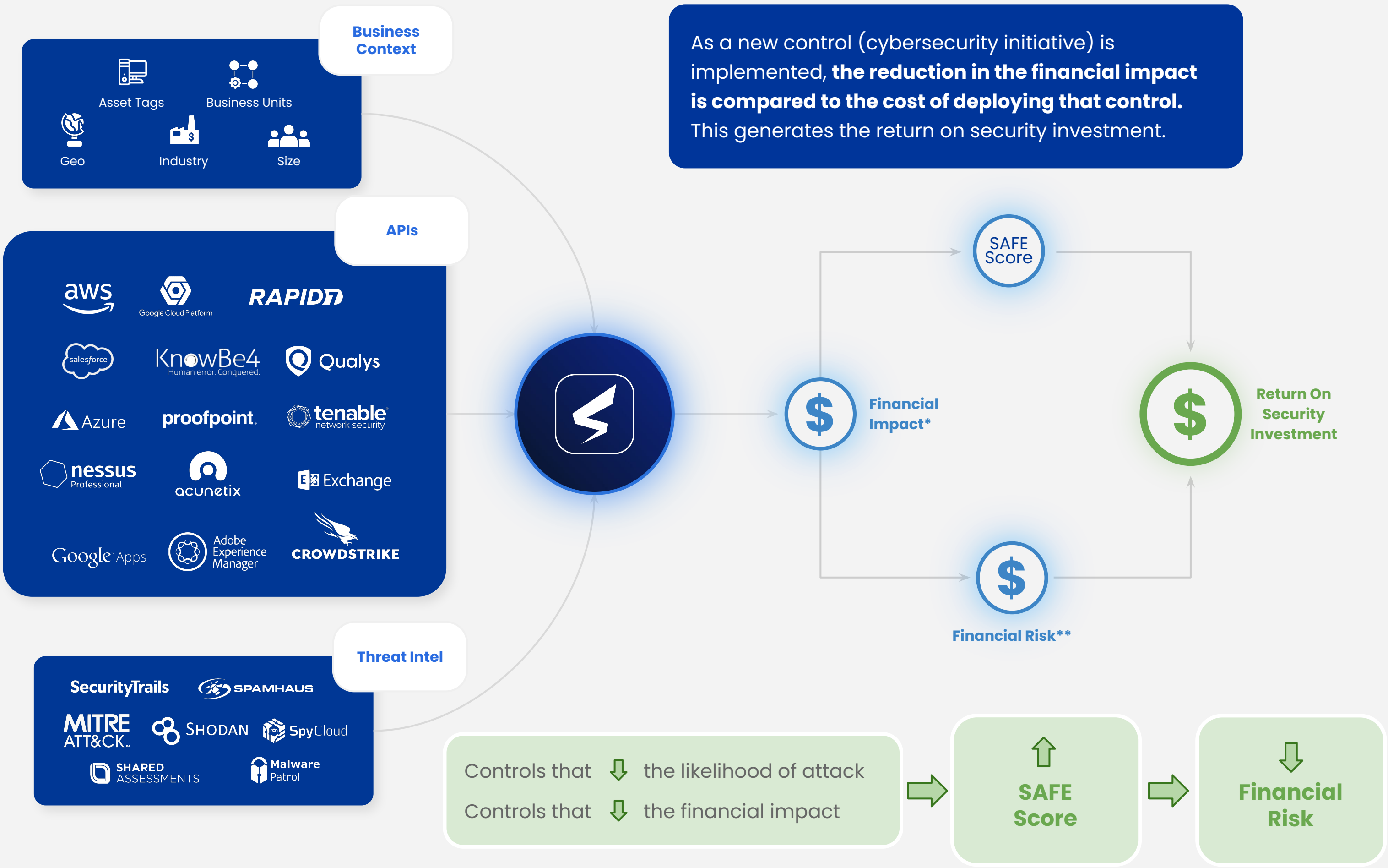
ENABLING TRUSTWORTHY CYBER RISK QUANTIFICATION AND MANAGEMENT

Establish financial risk reduction as the common denominator to understand the effectiveness of every cybersecurity investment your business makes

How the ROSI calculator outperforms other models on the market

Commercially available models	Safe Security ROSI model
✗ Manual and time intensive processes	✓ Automated signals-driven inputs powered by API
✗ Provide point-in-time and static assessments that date quickly.	✓ Produces dynamic outputs that are continuously updated in real-time
✗ Limited scope: Heavy focus on the financial impact of regulatory penalties.	✓ Gathers signals across people, processes, technology, compliance, and third parties
✗ Fail to assess cyber insurance while calculating the financial impact	✓ Includes cyber insurance as a control while calculating the financial impact
✗ Individual scenarios need to be created and analyzed separately	✓ Provides the analyses of multiple types of initial attack vectors on a single dashboard

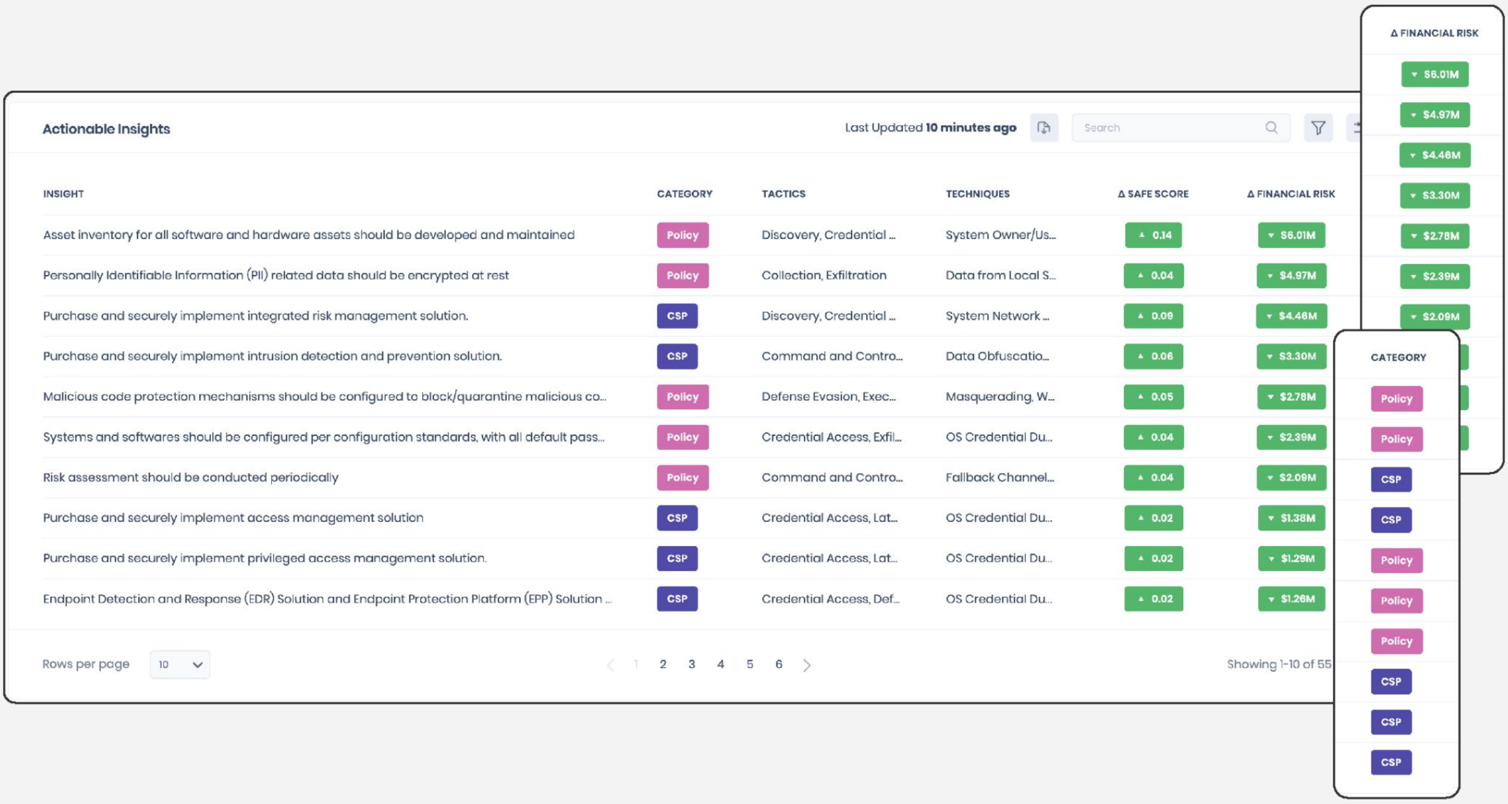
How does the ROSI module work?



As a new control (cybersecurity initiative) is implemented, **the reduction in the financial impact is compared to the cost of deploying that control.** This generates the return on security investment.

Financial Risk: The product of the estimated financial impact from cyber risk times the annual likelihood of that risk occurring.

** **Financial Impact:** The $ cost of one or more cyber attacks (were those attacks to happen); expressed by upper bound, expected, (mean), and lower bound values.



Actionable Insights

Last Updated **10 minutes ago**

INSIGHT	CATEGORY	TACTICS	TECHNIQUES	Δ SAFE SCORE	Δ FINANCIAL RISK
Asset inventory for all software and hardware assets should be developed and maintained	Policy	Discovery, Credential ...	System Owner/Us...	▲ 0.14	▼ $6.01M
Personally Identifiable Information (PII) related data should be encrypted at rest	Policy	Collection, Exfiltration	Data from Local S...	▲ 0.04	▼ $4.97M
Purchase and securely implement integrated risk management solution.	CSP	Discovery, Credential ...	System Network ...	▲ 0.09	▼ $4.46M
Purchase and securely implement intrusion detection and prevention solution.	CSP	Command and Contro...	Data Obfuscatio...	▲ 0.06	▼ $3.30M
Malicious code protection mechanisms should be configured to block/quarantine malicious co...	Policy	Defense Evasion, Exec...	Masquerading, W...	▲ 0.05	▼ $2.78M
Systems and softwares should be configured per configuration standards, with all default pass...	Policy	Credential Access, Exfil...	OS Credential Du...	▲ 0.04	▼ $2.39M
Risk assessment should be conducted periodically	Policy	Command and Contro...	Fallback Channel...	▲ 0.04	▼ $2.09M
Purchase and securely implement access management solution	CSP	Credential Access, Lat...	OS Credential Du...	▲ 0.02	▼ $1.38M
Purchase and securely implement privileged access management solution.	CSP	Credential Access, Lat...	OS Credential Du...	▲ 0.02	▼ $1.29M
Endpoint Detection and Response (EDR) Solution and Endpoint Protection Platform (EPP) Solution ...	CSP	Credential Access, Def...	OS Credential Du...	▲ 0.02	▼ $1.26M

Rows per page 10

Showing 1-10 of 55

Research

SAFE's ROSI calculation is powered by the Interactive Cost Model: its **Financial Risk** and **Financial Impact** values influence the return on security investments.

THE INTERACTIVE COST MODEL

The ICM is powered by **Safe Security's proprietary database** - built and maintained by our expert analysts and threat intelligence teams. The model leverages:

- Over **500,000 data points** across **2,000 mapped discrete incidents** taken from primary sources across financial fraud, ransomware, PxI data breaches, wiper and cryptocurrency theft, and data privacy violations.
- **~1300 CVEs** identified as seen in the wild., and **over 1,100 attack groups** including identified aliases.
- A pipeline of over 25,000 security incidents being actively reconciled and processed.

To provide the granularity necessary for default cost driver modeling, all discrete attack costs are mapped by:
:

- Incident mapped to timeline and attribution
- Entity attacked geolocation and revenues
- Parent attack type, sub attack type
- Campaign type and data source
- Direct or indirect cost
- PXI contents such as PHI, PII, PFI, and PCI
- Pre-attack cybersecurity posture
- Consent order details, if applicable, **and much more**

THE SAFE PLATFORM:

- **TTP mapping to MITRE ATT&CK** for over 140 attack groups and malware (with more added regularly)
- **Telemetry** from ~400K assets on our platform today
- **Hack analysis** of ~100 breaches over the last 3 years
- **Bayesian Network model co-developed with MIT and Douglas Hubbard,** President of Hubbard Decision Research. It calculates probabilities from bottoms-up of a successful attack happening within the next 12 months.

For more information, visit safe.security/safe/return-on-security-investment

Legal Disclaimer: The output generated by this cost model is purely indicative and based upon historical and publicly available research data. Safe Security takes no responsibility for the accuracy and correctness of these calculations and disclaims all liability in respect of any actions taken or not taken based on any contents of the cost model. We advise you to contact Safe Security for accurate results.