SAFE – GenAI Risk Management

Comprehensive Solutions for Managing AI Risks

With the rapid adoption of Generative AI (GenAI), businesses are exposed to new, complex risk scenarios. Understanding and quantifying these risks is essential to maintaining innovation without compromising security. Current AI adoption trends reveal several key challenges:

- **Unknown Risks**: Many businesses are unsure of how AI systems may introduce new vulnerabilities, leaving them exposed to unforeseen threats.
- **Lack of Quantification**: Quantifying the impact of AI risks remains a challenge for most organizations, making it difficult to prioritize risk management efforts.
- **Compliance Complexities**: As regulations around AI develop, organizations are struggling to align their AI practices with emerging frameworks like NIST AI-RMF, potentially leading to regulatory non-compliance.

SAFE Security addresses this challenge by launching the AI Risk Management module, empowering CISOs and risk analysts to manage AI risks proactively.

Why SAFE for AI Risk?

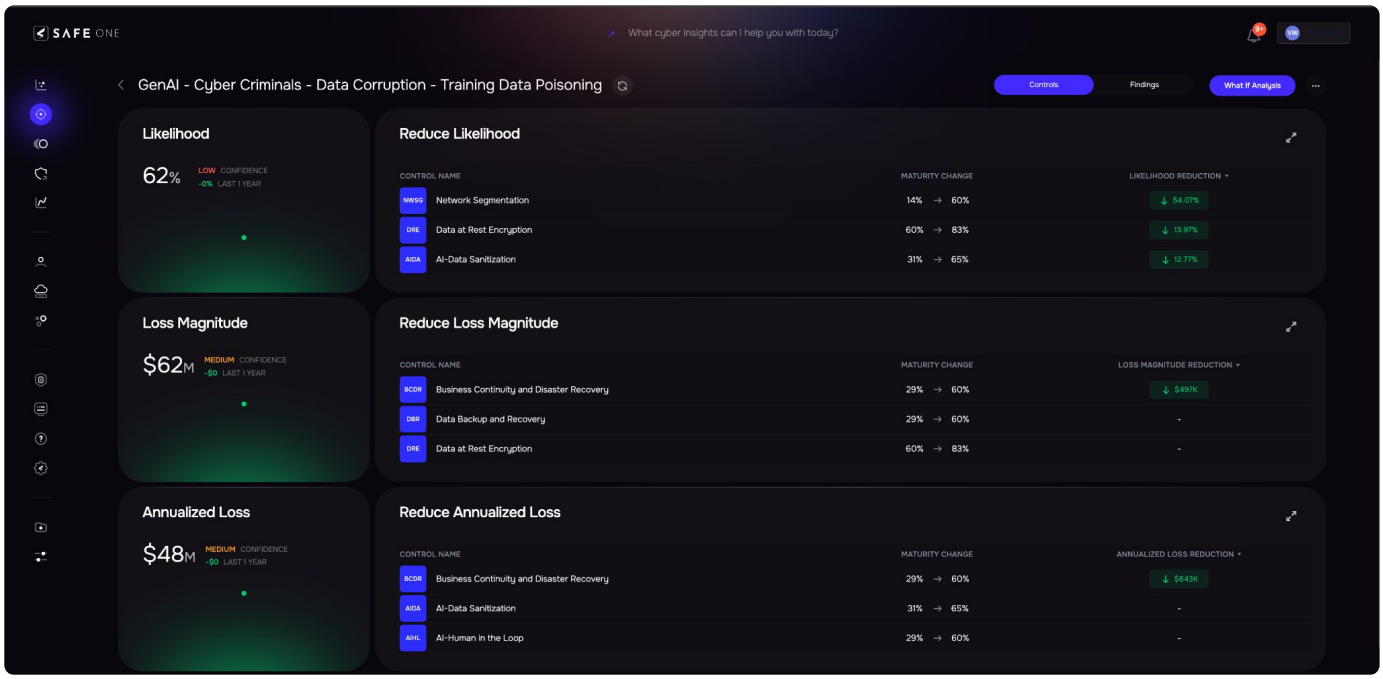
Tailored Risk Insights
Provides insights tailored to an organization's specific AI use cases, offering highly relevant risk assessments and mitigation strategies.

Comprehensive Risk Quantification
SAFE quantifies the likelihood and potential business impact of AI-related risks, enabling organizations to prioritize resources effectively.

Proactive Compliance Alignment
Aligns AI risk management practices with regulatory frameworks like NIST AI-RMF.

Real-Time Risk Visibility
Provides continuous monitoring of AI-related threats and vulnerabilities, through the Live Threat Center module

Through SAFE's GenAI Risk module, businesses can assess the likelihood of a breach and the potential financial impact of various AI risk scenarios. Users can model these risk scenarios based on resources like the MIT AI Risk Library and the Databricks DASF publication. Additionally, organizations can evaluate their AI risk posture using the NIST AI-RMF framework, ensuring compliance with regulatory standards. This AI risk management module is part of the Enterprise Edition of the SAFE One platform.



GenAI Risk: Capabilities

AI Risk Quantification

SAFE's platform enables organizations to quantify AI risks, offering an understanding of Breach Likelihood and Loss Magnitude for different AI-related risk scenarios. By calculating the financial impact of AI risks, businesses can better prioritize their cybersecurity investments and mitigation efforts.

Scenario-Based Risk Modeling

With access to the MIT AI Risk Library and other key resources like the Databricks DASF publication, SAFE's module allows organizations to model risk scenarios tailored to their specific AI use cases. Whether it's a data privacy issue or a breach involving AI-generated content, the platform provides detailed insights on the potential impact.

Automated Risk Scenario Information

Based on an organization's AI footprint and specific vulnerabilities, SAFE automatically generates AI risk scenarios. These scenarios help businesses understand the risks posed by specific hacker groups, AI-driven attack vectors, or vulnerabilities within their AI systems.

Real-Time Risk Monitoring and Updates

With Live Threat Center in SAFE's platform offers real-time updates on emerging threats and vulnerabilities related to AI.

AI Posture Evaluation

The SAFE platform helps organizations evaluate their AI risk posture using the NIST AI-RMF framework. This evaluation not only highlights potential vulnerabilities but also ensures that the organization's AI adoption aligns with industry regulations and compliance requirements.

GenAI Risk: Key Use Cases

Understanding AI Risks: AI is evolving quickly, making it hard to fully grasp its risks. SAFE helps businesses identify, assess, and manage these risks, enabling them to confidently move forward with AI projects.

AI Risk Insights for CISOs: CISOs need to understand how AI affects their organization's cyber risk. SAFE provides clear, quantifiable insights that help CISOs communicate risks to leadership and prioritize mitigation.

Ensuring AI Compliance: As regulations like NIST AI-RMF evolve, SAFE helps businesses align their AI practices with compliance standards, reducing the risk of penalties.

Confident AI Adoption: SAFE equips businesses with tools to manage AI risks effectively, enabling them to adopt AI confidently while balancing innovation with security.

SAFE GenAI Risk Management empowers CISOs with real-time, actionable insights to manage AI risks confidently while ensuring compliance with evolving regulations. By integrating AI risk management into the broader cybersecurity strategy, SAFE enables businesses to embrace AI innovation without compromising security or increasing exposure to critical threats.

Want to see SAFE GenAI Risk in action? Schedule your 1:1 demo with a SAFE cyber risk expert today.