VISO TRUST

TPRA 2024

AI Driving Broader, Deeper Nth Party Cyber Risk Assessment

Trading Up from Tradeoffs

Paul Valente | CEO & Co-founder, VISO TRUST

VISO TRUST

Today's Session:

- ➔ The State of AI & ML
- ➔ AI Breakthroughs & Limitations
- ➔ Third Party Risk: Opportunities & Challenges with AI
- ➔ Real-world AI-powered TPRM success stories
- ➔ Q&A

Definitions

- ➔ **AI:** Artificial Intelligence
- ➔ **ML:** Machine Learning
- ➔ **LLMs:** Large Language Models

The State of AI & ML

What is machine learning (ML): A type of AI where machines learn from data to perform tasks like classification and prediction

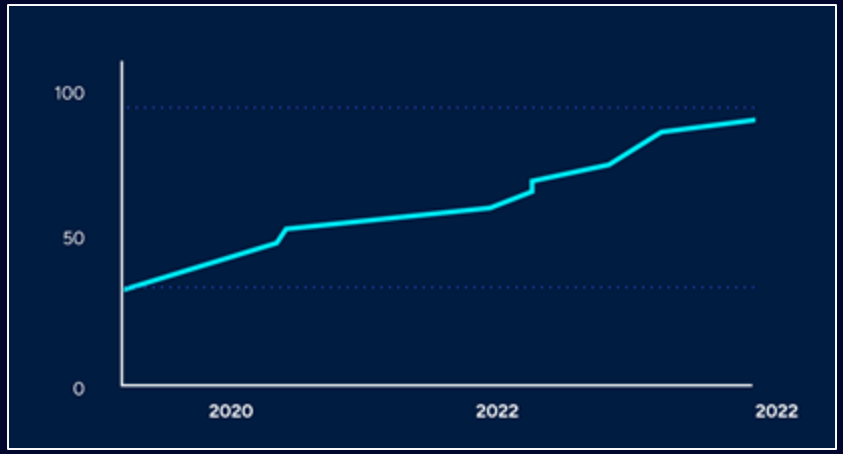
Three main types of ML:

- ➔ **Supervised learning:** Trains on labeled data (data with answers) to create models for tasks.
- ➔ **Unsupervised learning:** Discovers hidden patterns in unlabeled data.
- ➔ **Reinforcement learning:** Learns through trial and error, used for training AI robots or game-playing algorithms.

Breakthroughs with LLMs

- **Generative Capabilities:** Capable of generating text, images, video, content, research, etc.
- **Scaling & Efficiency:** Can follow prompts to complete tasks, check work, or collect information.
- **Conversational AI:** User input can improve a LLM's reliability and safety.

The Rise of Superhuman Capital



Data Source: Foundation Capital

Limitations with LLMs

- **Accuracy and Reliability:** LLMs can be unreliable at times, generating responses that are factually incorrect
- **Context Issues:** LLMs may struggle to grasp the nuances of language, like understanding the different meanings of a word depending on the context.
- **Bias and Fairness:** LLMs inherent biases from the data they're trained on
- **Misinformation:** There's a risk of LLMs generating misleading or factually incorrect information
- **Limited Creativity:** LLMs are better at remixing existing information than coming up with truly original ideas.

The Challenge

Complex and growing vendor ecosystems are **expanding the attack surface** for all businesses.

71%

of all software will be SaaS by 2026[1]

100%

of tech footprints will be third-party[2]

65%

of breaches are due to third party failures[3]

[2]Forrester, 2018: The Year Of Enterprise DevOps, 2018; Accenture, DevOps Adoption, 2018; Interop ITX, 2018 State of DevOps, 2018; Google, State of DevOps, 2019; Blissfully, 2019 Annual SaaS Trends Report, 2019; BetterCloud, State of the SaaS Powered Workplace, 2017; Cisco, Global Cloud Index 2018; Forbes, State Of Enterprise Cloud Computing, 2018; [3]Ponemon, 2019; CarbonBlack, 2019; Bomgar, 2018; Crowdstrike, 2018; Soha Systems, 2016; IBM, Cost of Data Breach, 2019; Forbes (Statista), Average Cost of Data Breach, 2020, Statista, Annual Number of Data Breaches in US, 2020

VISO TRUST

Third Party Risk: Complex & Growing Problems

Current assessment approaches are **expensive and slow**

Companies are forced to choose between **competitive advantage and security**

Staff shortages and **limited compliance expertise** are adding to security team challenges

How Existing Solutions Fall Short

Up to **75% of vendors** refuse to fill out questionnaires

90% of high severity findings are **false positives**

As much as **98% of reports are invalid**

Only **6%** of vendors can be assessed on public data alone

80% of security teams say they can't keep up

Questionnaire-based assessments take **60-90 days** on average

Up to **90% of CISOs** report high stakeholder frustration

Effective third party risk management is more than a safeguard--it's the ability to rapidly innovate while eliminating risk.

In short, it’s a competitive advantage.”

Alexander Hughes

Information Technology and Compliance Executive

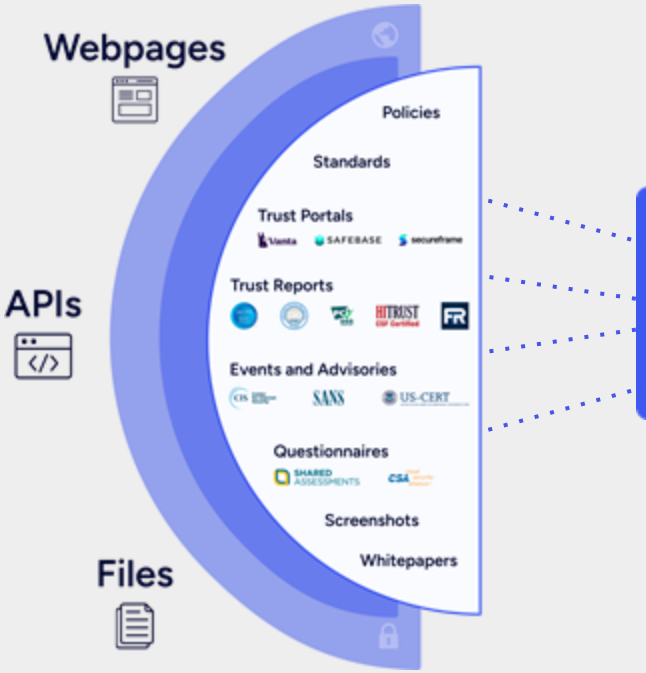
How can AI turn TPRM from “red tape” into a competitive advantage?

How to Win in Third Party Risk with AI

- → Reduce time to assess
- → Reduce manual work
- → Reduce risk
- → Maintain compliance
- → Scale

Building Comprehensive Risk Assessment with AI

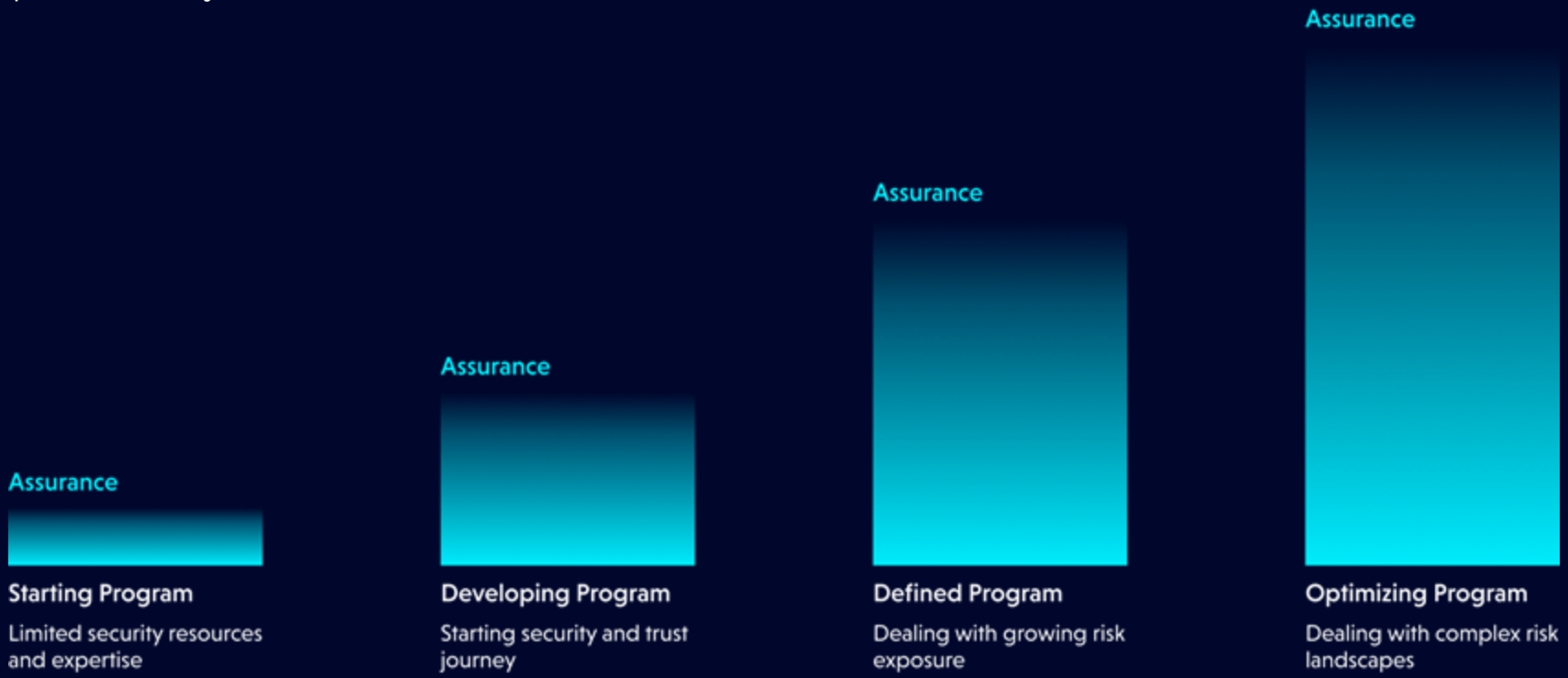
Aggregate data from diverse public and private sources.



Artificial Intelligence automatically discovers, classifies, and assesses relevant control information.

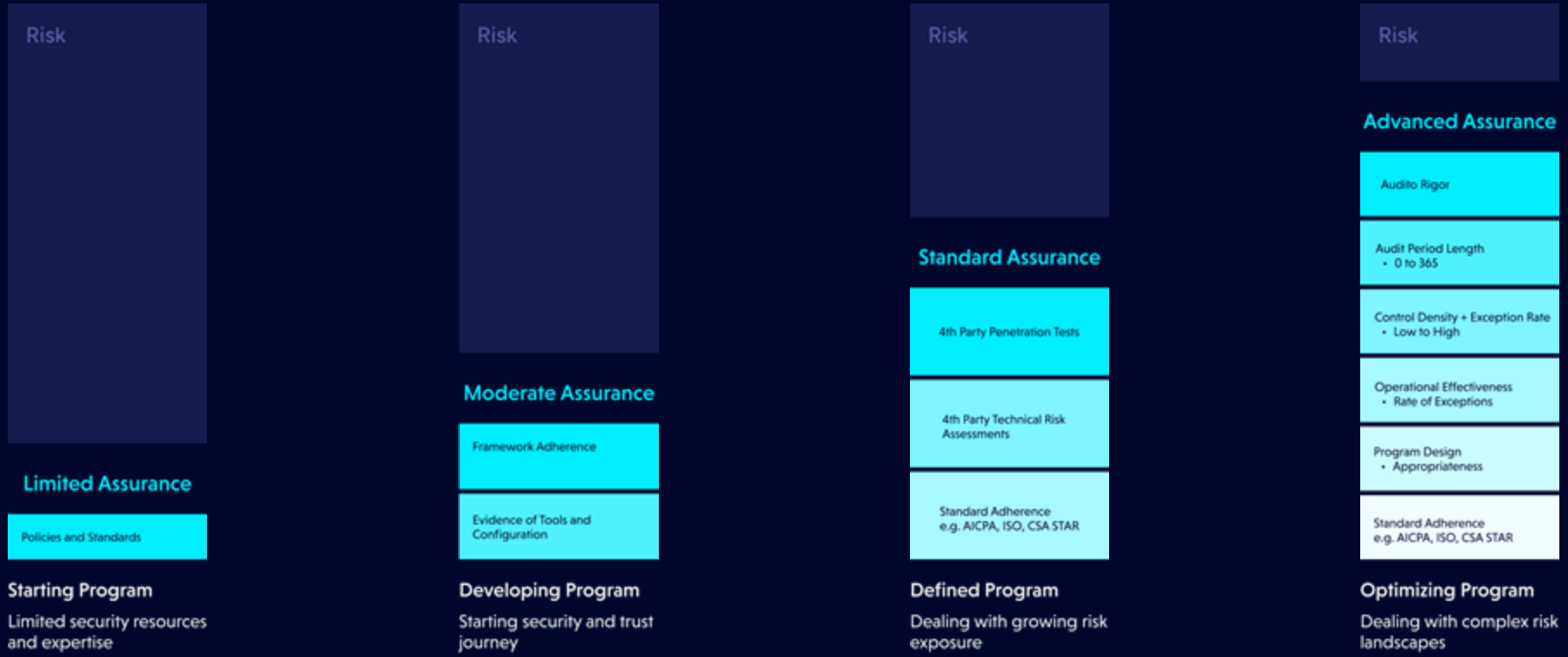
Security Program Maturity and Assurance

The more mature a security program becomes, the more assurance there is to their customers that the frequency and impact of security incidents will be minimized.



Building Comprehensive Risk Assessment with AI

You can measure this assurance and accurately and flexibly determine risk.



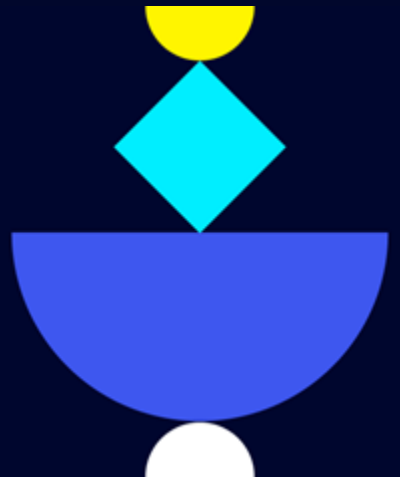
High Level Use Cases Required

- ➔ Automated Inherent Risk Calculation
- ➔ Automated Artifact Analysis
- ➔ Automated Control Categorization and Analysis
- ➔ Automated Population of Questionnaires
- ➔ Framework Handling
- ➔ Control Effectiveness Determination
- ➔ Assurance Determination
- ➔ Residual Risk Determination
- ➔ Nth Party Identification
- ➔ Public Resource Monitoring - Entity Matching and Risk Determination

Sample Use Case

Analyzing a SOC Report

- ➔ Identify and classify artifacts
- ➔ Detect standards
- ➔ Validate scope
- ➔ Analyze Auditor Opinion
- ➔ Detect audit period
- ➔ Determine validity
- ➔ Identify exceptions
- ➔ Detect subservicers
- ➔ Determine audit rigor
- ➔ Calculate control density



What's Required to Build

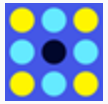
- ➔ Open Source and Proprietary AI Tools and Infrastructure
- ➔ Sr. Software Developers with AI Experience
- ➔ Sr. Machine Learning Engineers
- ➔ Sr. Security Architects
- ➔ Sr. Risk Architects
- ➔ Sr. Auditors w/ Specific Framework Experience
- ➔ Training Data - Tens of thousands of artifacts of each type, to train across 25+ frameworks & 100s of artifact types

What Companies are Achieving with AI

Notion instacart upwork Commonwealth illumio

<5 mins

Spent per assessment



5-7 days

Average time-to-assess

↑ 98.4%

Response and completion rates

↑ ↑ ↑

Higher coverage and accuracy

96%

Less work

↓75%

Risk exceptions and acceptance

25x

More risk vendors caught

↓95%

Reducing risk from third-parties

VISO TRUST

Commonwealth

“ Without AI, **I was going to need 3 more analysts - going with an AI solution was an easy decision** that made perfect sense.”

Kevin Donis
Information Security Risk Lead

Critical Business Issues

- Time consuming, unscalable and **very manual assessment process**
- Lack of standardized processes and continuous tracking
- **Low visibility** into vendor population

Solution Requirements

- **Centralized solution** for tracking risk data
- Quickly assess new vendors, **unblocking the procurement process**
- Solution needed to **automate at scale**

Results with AI for TPRM

- Expedited the vendor assessment process from **6-8 weeks to 1-2 weeks**
- Allowed the team to start assessing potential vendors allowing the Security Team to help **influence the buying decision.**
- Within **6 months**, the onboarded vendor network was able to **double**
- Built trust and cooperation with vendors by providing an **easier painless process**

VISO TRUST

Global Financial Services Firm

"What's really amazing is the accuracy. AI provides everything we need to know to make qualified risk decisions."

Critical Business Issues

- **Unable to assess and onboard** third-party vendors consistently with existing solution
- Unfortunately in 1 year, they **assessed less than 33% of the required population**

Solution Requirements

- Centralized view of their large partner ecosystem
- Ease of use for third-party vendors and partners
- Accelerate and onboard all of their contracted vendors
- Ability to quickly implement the new solution

Results with AI for TPRM

- In one month, assessed **2x more than the previous solution was able to deliver in 1 year**
- Empowered the team to make qualified risk decisions across their entire vendor footprint
- **8x** completed assessments
- Decreased time spent on assessments from months to days; **average assessment completed in < 2 weeks**

VISO TRUST

cruise
a subsidiary of General Motors

"AI has completely automated the process, reducing staff expenses by 90%, time to completion by 50% while supporting 117% more vendor assessments."

Alexander Hughes
Information Technology and Compliance Executive

Critical Business Issues

- Rapid growth of the organization led to increasing assessment demands
- Not enough security staff to cover the growing backlog
- Existing process was labor intensive and frustrating for stakeholders and vendors

Solution Requirements

- Assist the team in getting through the growing back log
- Leverage automation where possible to allow their team to keep up
- Provide quality risk data and reporting

Results with AI for TPRM

- Cruise is able to complete **117% more assessments per month**
- **Improved employee morale** by automating the manual processes so the security team could focus on their core tasks.
- **Reduce overall risk** through quality and consistent insights
- Reduced rate of security **exceptions by 75% while detecting 5x more risky vendors**
- 100% of the backlog was **eliminated in the first 60 days**

Choosing a Trustworthy Third Party Risk Provider

Reduce Risk

- Choose an established and trusted vendor
- Vendor has a trustworthy approach to AI

Drive Operational Efficiency

- Look for patented AI technology
- Choose a solution that supports frameworks, regulations, and standards that your business needs

Fast Track Your Business

- Company that has expertise, data, third party audit experts, and models to deliver with precision

VISO TRUST

Paul Valente
CEO & Co-Founder of VISO TRUST

Paul is a former CISO in highly regulated technology companies and has helped 250 of the Fortune 1000 improve their TPRM programs

EMAIL
paul@visotrust.com

Connect with us!

Visit us at Booth #11

Website:
www.visotrust.com

VISO TRUST

Q&A!

- ➔ Raise your hand
- ➔ If you’re thrown the ball, ask your question!