Forgepoint

2024 Q4 Report

/ Forgepoint Forward /

What's Ahead in AI Governance

Table of Contents

2	Introducing Forgepoint Forward
3	The State of AI Governance
4	Challenges
6	Opportunity for Startups
14	What Executives Want: Areas for Opportunity
17	Final Thoughts and the Future of AI Governance
18	Acknowledgements
20	Endnotes

> *AI Governance is about establishing frameworks that ensure greater visibility and accountability over AI usage and adherence to internal and regulatory standards and policies. This includes AI discovery, monitoring AI systems, and generating policies that guide the deployment of AI across the organization in a way which is more dynamic to changes in how the application is being used."*

Elena Kvochko

Adjunct Professor, Cornell University
SC Johnson School of Business

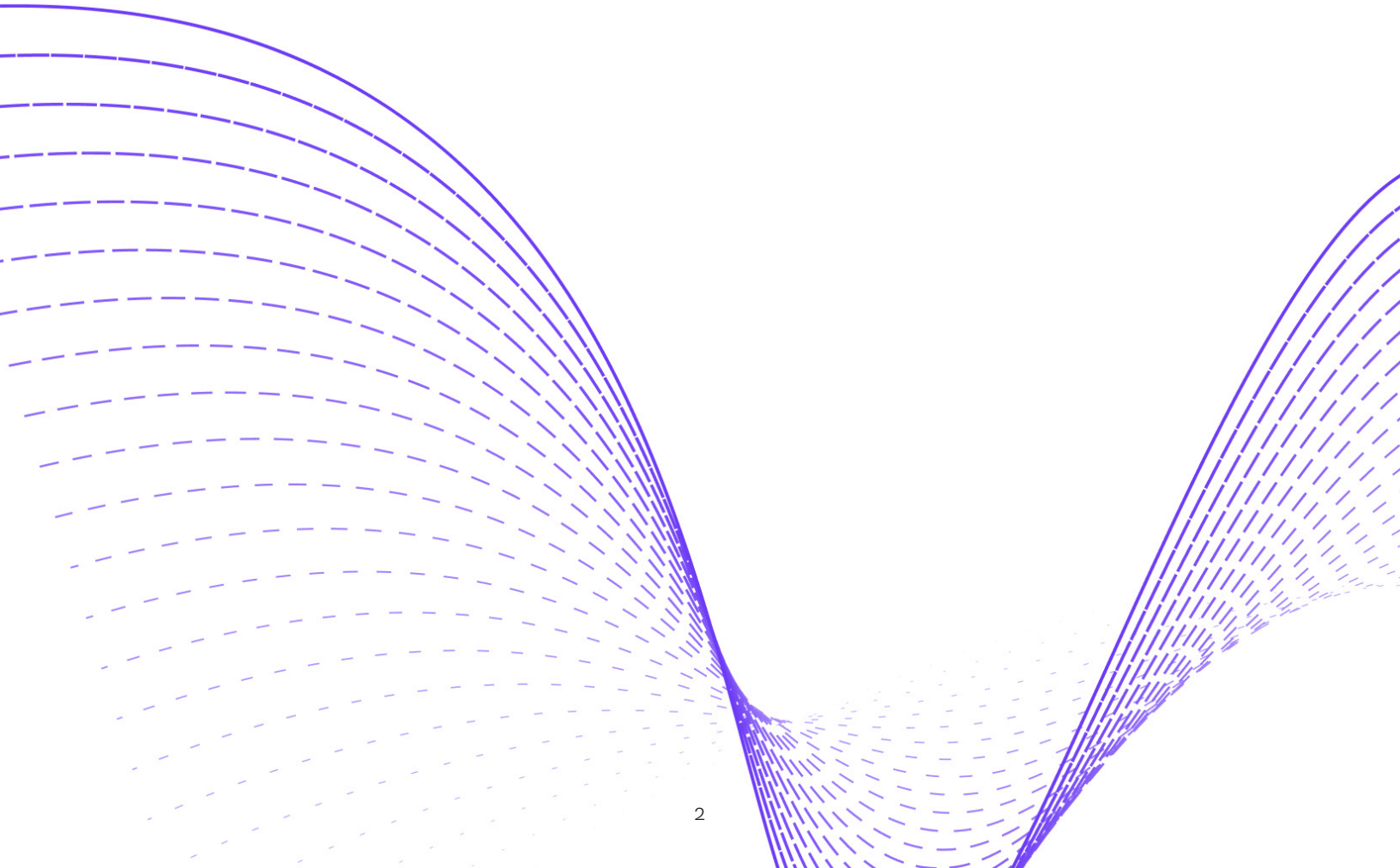
Introducing Forgepoint Forward

In today's rapidly evolving digital landscape, the role of cybersecurity has never been more critical. Modern companies navigate a complex threat environment, often relying upon big tech partners and legacy solutions, but still face critical security gaps. These gaps represent risks and opportunities – the linchpins of cybersecurity innovation, software development, and economic progress.

As longtime investors, operators, and company-builders with decades of experience in cybersecurity, the Forgepoint Capital team has the privilege of collaborating with a deep network of CISOs, CIOs, CEOs, industry experts, and national security leaders. These individuals are at the forefront of defending against cyber threats, implementing robust security postures, and fostering organizational and industry resilience.

What follows is the second edition of Forgepoint Forward, a series of quarterly reports on the most critical emerging spaces in cybersecurity, artificial intelligence, and infrastructure software. Forgepoint Forward presents our findings from extensive research and interviews with experts across our network-including our Global Advisory Council. Our goal is to highlight investment trends and market projections, as well as startups involved in promising areas, to identify key opportunities for entrepreneurs and technology leaders across the cybersecurity community.

We would like to extend our thanks to everyone in our community who shared their insights and contributed to this report. A full list of contributors can be found at the end of this report under Acknowledgements.



The State of AI Governance

The recent explosion of generative AI (GenAI) technology and its seemingly exponential rate of change is altering modern business operations. As enterprises across nearly every industry increasingly evaluate and integrate new AI models, a mix of excitement and concern permeates executives' mindshare.

On the one hand, AI models introduce new internal process automations, assisted decision making, and opportunities to boost personal productivity across business functions. Workers may seek out numerous Generative AI tools to create content or Large Language Models (LLMs) to perform menial tasks. 25% of the use cases involve content creation, such as editing, summarization, translation, while another 18% are business tools that help enhance workplace productivity.[1] In these cases, the use of the tool is easier to gauge from the nature of the provider.

On the other, there are persistent risks including hallucinations, bias that creates unfair outputs, and sensitive data leakage. At the same time, AI model attack surfaces continue to grow alongside their capabilities.

What concerns do CISOs have regarding AI Governance?

As a result, securing AI model usage and development have become top-of-mind issues for CISOs. There is an urgent need for AI Governance- guardrails that ensure AI tools are secure and ethical- across business functions. Boards, executives, and senior leadership must establish AI governance policies and practices while audit and legal counsel ensure compliance with internal standards, contractual requirements, and industry regulations. Security teams search for solutions that improve security posture and mitigate AI risks. Amidst the shifting AI governance landscape, one thing remains clear: companies are acting on the need to implement robust governance frameworks and security tools that operationalize responsible and compliant AI usage and development practices to proactively manage modern enterprise risk.

> *"The attack surfaces of these models are growing in a way that people do not understand. The more functionality and capabilities they have, the larger the attack surface. These issues require a risk mitigation plan – it is not a matter of if, it is a matter of when."*

Tobias Yergin

Head of Product, Strategic Exploration, Fortune 50 Retailer

Challenges

1) Employees are using AI without oversight or approval, introducing invisible risks across multiple attack vectors.

With the rapid adoption of AI tools and applications, many companies lack the capability to comprehensively track and manage employee usage. Most companies lack the fundamental capability to track and manage how employees use AI tools and applications. Shadow AI is becoming a more significant problem as employees choose to use unauthorized SaaS-based GenAI tools instead of approved or in-house models, contributing to SaaS sprawl (the uncontrolled use of SaaS applications in organizations)[2]. This trend exacerbates enterprise software supply chain risk as each new AI application introduces its own set of third-party software components and data sharing and model training concerns. Many public AI tools appear to be offered by small companies that act as a proxy for core providers of foundational models which may have questionable security and privacy controls. Furthermore, some AI models may be trained based on customer data- a July 2024 report from Harmonic found that 30.8% of the AI applications employees were using declared that they train on customer data.[1]

Unfortunately, many companies have reacted to this widespread misuse by simply blocking access to GenAI tools outright. JP Morgan Chase and Verizon were two of the 25% of organizations that implemented GenAI bans over privacy and security concerns, as surveyed in Cisco's 2024 Data Privacy Benchmark study[3]. Bans on GenAI not only undermine potential productivity and automation advantages, but also serve as inefficient means of to implementing AI governance, as employees can circumvent these measures by using personal devices or other back doors. Imposing absolute restrictions can makes discovering AI application usage more difficult in the long term.

> *"CISOs around the world have been asked by their board or audit committee, 'What AI technologies are my employees using?' and very few can answer that with consistency and accuracy. Every day employees are making trust decisions about corporate data with third parties that IT and Security are not aware of. Employees are just looking for a new shiny tool that is going to make them more productive- they are not making effective security assessments."*
>
> 
>
> Russ Spitler
>
> CEO and Co-Founder, Nudge Security

CEOs and senior leadership may choose to invest in employee training to help mitigate unauthorized AI usage. However, the issues of maintaining holistic visibility over the AI applications, and vetting model security persist. Beyond visibility, scaling internal policies and procedures for AI utilization is also an immediate concern.

2) How do companies build AI models and implement AI technology in a secure manner?

Another concern executives have is around gaining visibility into the performance and behavior of models that are being developed and deployed in-house. Traditionally, ML engineering and operations teams monitor behaviors manually by tracking output accuracy and checking for anomalies, drift, and hallucinations, among other metrics. The modern enterprise requires real-time insights into model performance and risks, in addition to checks which prevent harm. This is essential to building and maintaining trust: companies must internally confirm that in-house AI models are ethical and responsible, and effectively communicate this externally as they acquire and retain customers.

A large part of monitoring AI software involves maintaining data governance, another high priority for CISOs. This includes confirming how data is being utilized, determining whether it is structured/unstructured data or internal/third-party data, identifying where it resides on-cloud or on-premise, and conducting data augmentation and synthesis. Quality assurance, access control, and compliance with data privacy regulations are also important aspects of data governance for AI models.

In addition to performance and robustness, transparency and fairness have emerged as key evaluation criteria for AI models. Models must be transparent and fair to gain trust. However, explainability– the ability to communicate how a model generated an output– is often difficult to establish. Explainable AI is an emerging governance discipline which aims to clarify how AI models make conclusions and hold model providers accountable for outputs (applying to in-house, open-source, and closed-source models).

> *"If you ask the people who have built the transformer architecture to explain to you how it works, they cannot. You must be careful because the depths to which things are explainable are a moving target... There should be a level of confidence associated with the model outputs, and if that confidence is breached the LLM should acknowledge it is not a high confidence score."*

Tobias Yergin

Head of Product, Strategic Exploration, Fortune 50 Retailer

Opportunity for Startups

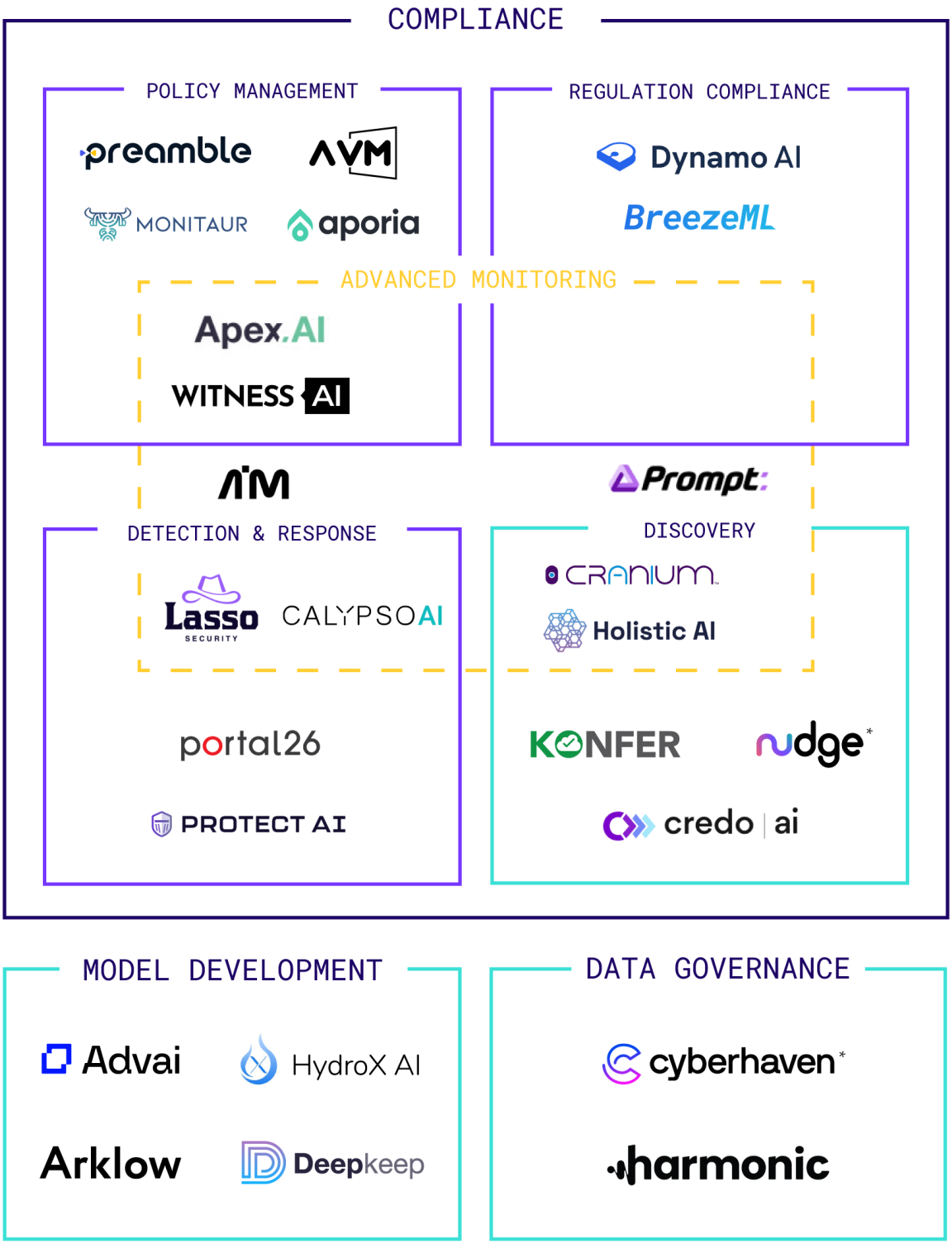
The variety of AI Governance segments has led to the emergence of startups that solve specific pain points around AI usage and development. We have mapped the current AI Governance startup landscape below, categorized by commercial focus or target functionality. Note that this landscape is constantly evolving as companies adapt to growing AI governance needs.

> *Everyone wants to capture the opportunity in this space. The name of the game is, they can't seem to spend enough on AI development. From a security perspective, companies want to enable AI and empower it but ultimately remain responsible for setting up the guardrails. Until they are able to manage the guardrails and set the governance, one might be a laggard."*

Brian Barrios

VP and CSO, Southern California Edison

AI Governance Market Map



Forgepoint

** = Forgepoint portfolio company*

AI Governance Market

Here is how we define each of these categories:

1) Compliance startups enable companies to adhere to internal company policies and applicable regulations. They often assist enterprises in generating compliance policies, identifying compliance gaps, and creating employee AI usage reports for executives. Some startups in this space also perform risk assessments to provide a governance score or design specific policies for their customers to implement.

2) Monitoring startups govern company employees' usage of and interactions with AI tools, models, and applications to ensure interactions with public AI technology are safe. Active monitoring tools can include the capability to audit data received from Gen AI providers for bias, create alerts to identify prompt injections and jailbreaks, and define data authorization boundaries.

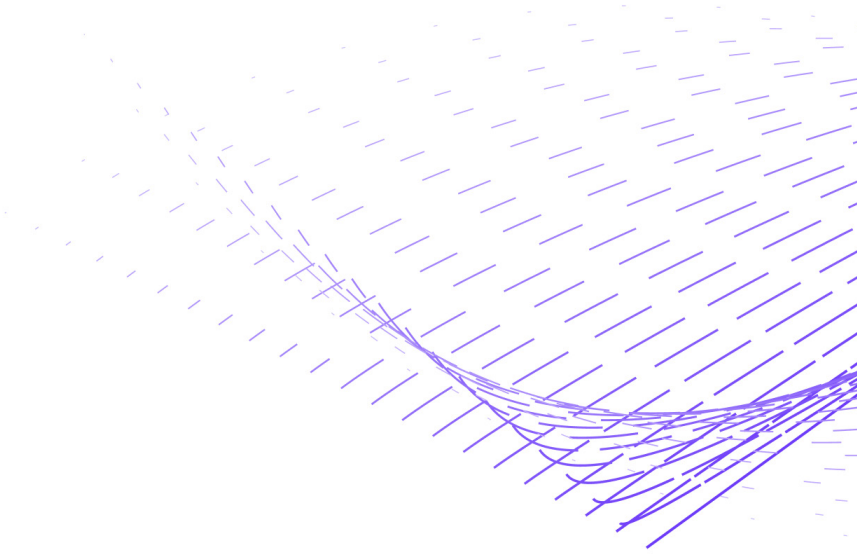
3) Detection and Response startups investigate GenAI incidents, conduct historical audits, and log employee interactions with AI models or tools. They take a more active role in blocking the entry of personal identifiable information (PII) and sensitive data prompts. These companies also evaluate how GenAI applications are used in company environments to identify vulnerabilities and understand performance.

4) Discovery startups help organizations gain a centralized view over which AI tools their employees are using and visualize information on adoption trends. By offering insights into the provider and the nature of the AI functionality and technology, these solutions help control the use of AI in the organization. Taking a human-centric behavioral remediation approach, these tools vet AI service providers and provide trusted tools for employees to use.

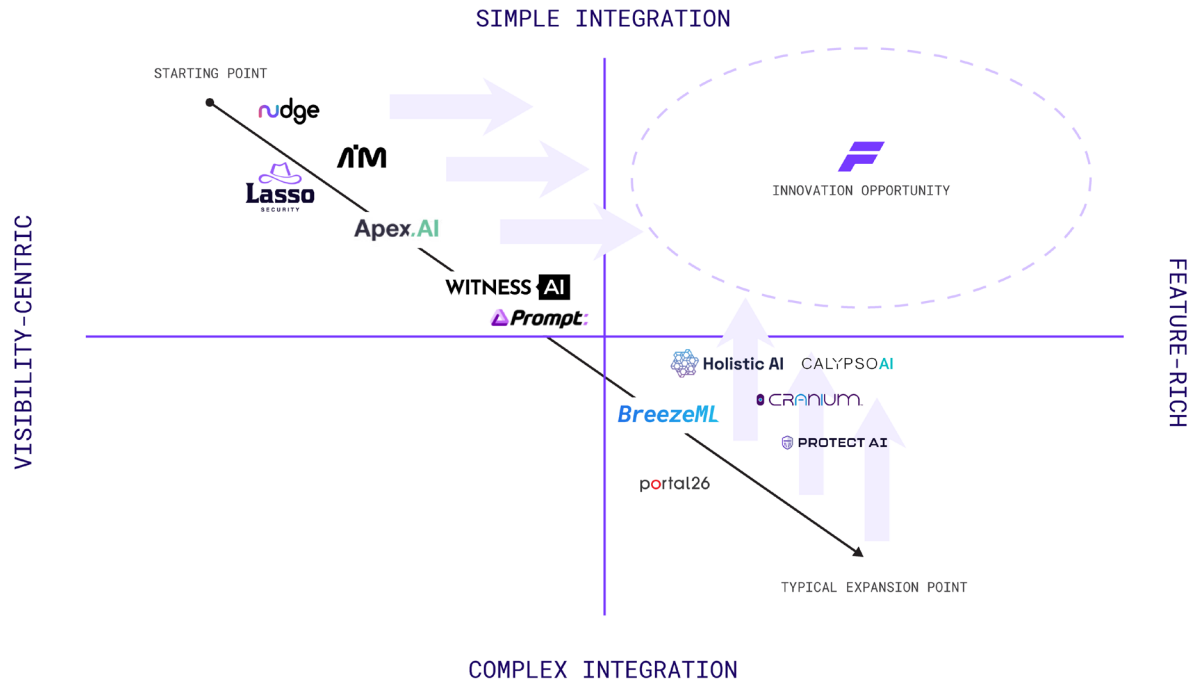
5) Model Development startups automate stress-testing or red-teaming and help companies conduct prompt validation to evaluate AI systems. Some providers may organize these findings and provide higher-level insights about model performance through a platform. These tools are designed more for data scientists or ML engineers than security teams.

6) Data Governance startups focus on the data element of AI Governance. Key functionalities include data leakage prevention, data loss prevention, visibility into how data is stored and flows into AI tools, and detecting and stopping sensitive data from being fed to Gen AI tools.

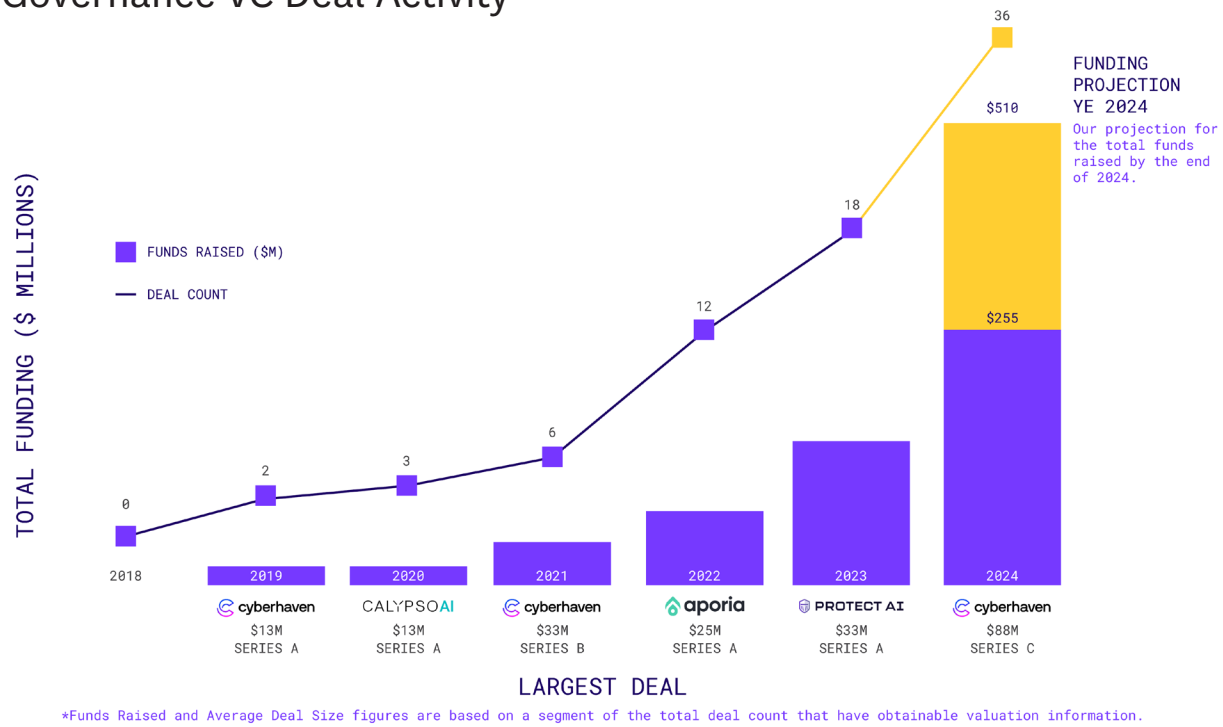
There is an interesting trend in the subset of startups who operate at the intersection of two converging spaces: **AI Governance and AI Security.** Several of these companies are using AI visibility as a starting point before expanding their feature sets horizontally or vertically. In doing so, their solutions tend to become much more complicated to integrate from a buyer's perspective. The startups that can add high value features while maintaining simple integrations will be in high demand.



AI Governance and Secuirty for AI Convergence: Value Propositions



AI Governance VC Deal Activity



*Funds Raised and Average Deal Size figures are based on a segment of the total deal count that have obtainable valuation information.

The growth of the AI Governance market and demand for governance solutions has been reflected in venture capital (VC) investments. Funding for AI Governance startups has grown every year since 2018 and is expected to continue increasing, both in terms of deal volume and value, as shown above.

Trends

1) Evolving Regulatory Landscape

As with most new technologies, the proliferation of AI has given rise to emerging regulations, frameworks, and restrictions.

These apply to both core LLM providers- managing ethical development and model risks- and AI-enabled use cases. There are also ongoing concerns around how existing data privacy regulations (like GDPR) and personal information HIPAA laws will influence pending regulations.

There are several emerging universal frameworks for AI Governance including the NIST AI Risk Management Framework[4], the OECD Principles on Artificial Intelligence[5], and the European Commission's Ethics Guidelines for Trustworthy AI[6]. On the regulatory front, the EU AI Act[7] is the first comprehensive AI-specific law to be adopted (going into full force in 2026). The AI Act sets reporting obligations for companies developing AI systems on the EU market and identifies high-risk AI use cases, requires risk management measures, and mandates the use of unbiased, high-quality training datasets and user data in compliance with the General Data Protection Regulation (GDPR)[8]. This legislation is expected to set a global standard, sparking similar regulations across the US and Asia that push more companies to adhere to standard AI governance practices.

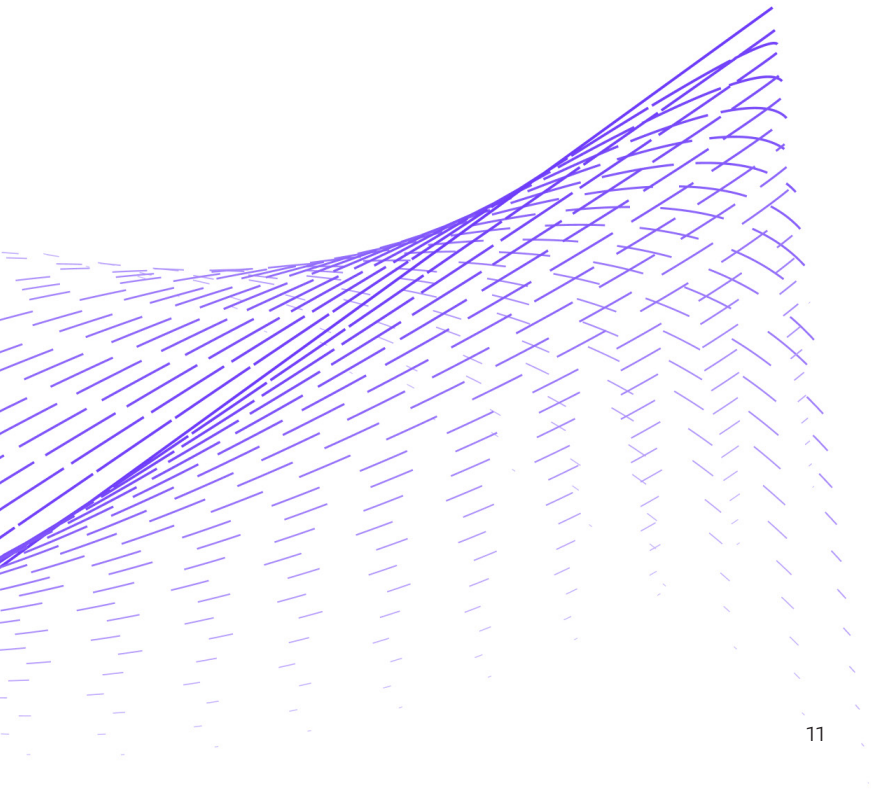
> *"The majority of AI systems at the moment use third party libraries and open-source code in their model. To be compliant with the EU AI Act, you need to be able to certify the model outcomes, how they have been trained, and make sure that it is unbiased, including the open-source part. In more business-related models (usually high-risk AI systems), it's extremely difficult to comply with all the requirements, since you cannot ask the open source to provide you with evidence of fairness or any certificates."*

Hazel Diez Castaño

Global CISO, Santander

The growing interest in AI regulations is expected to heavily impact industries like healthcare, financial, and national defense where AI outcomes carry higher levels of risk. Organizations which face heavier AI regulations may benefit from industry-specific compliance capabilities offered by AI Governance tools, such as the ability to generate compliance policies in accordance with regional or industry-specific regulations.

However, in the US, the future of AI regulations is less clear after the Supreme Court's recent Loper Bright Enterprises vs. Raimondo decision which overrules the precedent set by Chevron U.S.A Inc. v. NRDC around federal agencies' interpretations of ambiguous federal laws[9]. US Congress can no longer set basic rules which regulatory agencies interpret and administer as policies for specific circumstances (such as applying general mandates around privacy or trust to AI). This means that specific AI regulatory guardrails must be designed by Congress. In practice, this will make effective AI guardrails nearly impossible to pass and enforce, given the slow pace of legislative processes and the high speed of technological developments. There is also a higher risk of AI guardrails being poorly designed and only suited for yesterday's AI systems. In this weakened external regulatory climate, individual companies must set their own strong internal policies and frameworks around AI governance- and they need guidance to do so. Tools centered around AI governance can bring significant value to these companies.



> *"European regulators are much further ahead – notably, the AI Act in the EU shows that we are going to see other markets, such as the ASEAN countries, step forward and begin to regulate AI in the way that the US may get dragged into doing."*

> *"In the US, post-Chevron decision, it is going to take a long time to get any cyber regulation that matters. We're going to need some big AI imperative or impact, or attack that uses AI that makes us all come together. The impact of Chevron will unfortunately be felt for years and decades to come. I don't have faith that we will see a lot of regulations because our hands are currently tied."*

Evan Wolff

Partner and Co-Chair, Privacy and Cybersecurity Group, Crowell and Moring

2) Nascent AI Governance Team Structures and Budgets

Companies' budgets for AI Governance solutions are still maturing. Buyers do not typically have an allocated budget for governance tools like they might have for AI development or third-party AI models. However, we expect that that to change in the near future, particularly as more companies establish line items for AI visibility dashboards.

Given that governance-specific AI budgets are still materializing, the pace of technology development in this space currently outpaces demand. While aspects of AI that clearly drive business value- like model deployment and machine learning tools- are certainly top-of-mind and top of budget for CISOs (particularly in companies with lower headcounts and small IT teams) governance spending lags behind. Prospects are often happy to engage in a proof of concept but when the time comes to buy, they prefer to implement aggressive usage policies or bans instead of purchasing on a sophisticated governance tool. While many AI Governance startups have yet to gain significant traction despite the high degree of mindshare, there are promising candidates emerging.

> *I do not expect a new function for AI Governance, but companies will incorporate security practices for LLMs in their existing infrastructure, which will require new skills, new people, new processes, and new integrations. A lot must change, but I don't see it sitting outside the security organization. It is a new practice within it, and there may be new leadership at a fairly high level."*

Tobias Yergin

Head of Product, Strategic Exploration, Fortune 50 Retailer

> *You have to get the right people in the room. You have to have the legal team. You have to have business leaders. You have to have our compliance teams. PwC coined the term fusion center. AI governance is very much like that. You have to bring all the right people together so that we can innovate, experiment, and then eventually drive a big differentiator in our business, products, and capabilities."*

Eddie Borrero

CISO, Blue Shield of California

Aside from budgetary priorities, many companies are still figuring out how to structure their teams around AI Governance. There is room to drive more demand as these teams formalize. Larger companies that have several legal and compliance teams tend to view AI governance through a legal and governance, regulation and compliance (GRC) lens while smaller companies may see it as more of a technical issue. The topic often brings together various teams including security, IT, HR, and auditors, with some starting to question whether they need a new operational or departmental function around AI. No matter how AI governance ends up fitting within organizational charts, it will clearly be a collaborative effort given the various aspects, uses of, and impacts from AI.

> *AI should not be owned or led exclusively by security. AI usage, AI governance means a higher-level cross collaboration decision. Multiple leaders should have a say in multiple aspects about how we're going to use, deploy, and monitor AI."*

Christie Terrill

CISO, Bishop Fox

3) Using Multiple AI Governance Tools within a Responsible AI Stack

Given the high concentration of point solutions in the market, buyers have an opportunity to take advantage of synergies between AI Governance tools. For example, a discovery tool from a provider like Nudge can easily co-exist with monitoring capabilities from companies like CalypsoAI that observe and secure LLMs and AI applications.

Part of the reason for the current proliferation of point solutions is that the market is not very mature yet, and the tools which solve specific pain points are actually adding the most value for customers. The value generated from more general platforms tends to be more dependent on the input from the user and may be less useful currently.

> *I have seen applications and efforts to secure AI and provide governance that are very smart. They customize access policies around AI, can be enforced on an automated basis across the enterprise, and trace information from the AI model's source to the output. These are tools that remove the input-based, manual work of discovering where across the enterprise you use AI."*

Elena Kvochko

Adjunct Professor, Cornell University
SC Johnson School of Business

What Executives Want: Areas for Opportunity

1) AI Governance solutions that build trust in AI

Executives' stances on AI exist on a spectrum between caution about how to proceed with adopting AI and fear of missing out on the efficiencies and business value that AI can enable. These perspectives are driving executive leadership and boards to gain a fundamental understanding of how AI models and governance solutions work. The ambiguous nature and lack of transparency around many AI applications has made some companies distrust startups with lower traction when compared to mainstream providers and larger vendors. CISOs with this concern believe that the trusted software or infrastructure providers they already partner with will catch up and develop AI applications and capabilities to safeguard AI.

> *"We are patiently waiting for our existing platforms to integrate AI capabilities and AI monitoring capabilities. We already trust them with sensitive data and they are already integrating various AI capabilities that sit on top of those platforms."*

Christie Terrill

CISO, Bishop Fox

On the other hand, many companies are ready to ride the AI wave and embed the technology in their environments. They may find that the focused AI Governance tools offered by many startups are a better fit.

In all cases, CISOs are also looking to also validate if AI tools are trustworthy, secure, and compliant with established policies given the critical role they can play. This is where AI governance innovations can step up. For example, governance tools might verify whether user inputs are secure according to data privacy and other compliance policies within an organization, preventing confidential data from being used for model training purposes. As third-party SaaS providers integrate AI into their services, AI usage might even become unintentional in some cases, making third party risk assessments and SaaS security offerings more relevant. Fundamentally, these security and governance practices can help strengthen trust and alleviate inordinate fears about AI.

As conversations around AI risk become more nuanced, CISOs may gravitate more toward startup point solutions- as long as the provider is trustworthy and has a strong reputation and customer testimonials.

> *"A lot of AI-powered applications, or the large language models that power those applications, are considered the crown jewel of a company. If a startup comes in to govern your crown jewel but hasn't yet figured out their data and trust policies and doesn't have transparent trust white papers explaining what they're going to do with your data, then I understand the hesitation."*

Elena Kvochko

Adjunct Professor, Cornell University
SC Johnson School of Business

2) Tools that help redefine training and awareness in the realm of AI usage

Employee behaviors are at the heart of technology adoption in business. No matter what tools an organization vets and approves for use (or blocks), employees have always found workarounds or shortcuts to get the job done- potentially exposing their employers to larger risks in the process. AI is the newest technology that can be misused.

> *Regardless of having monitoring tools or governance tools, there are always going to be workarounds. You must evaluate the value of the data that you're looking to protect, and consider how much you need to add monitoring tools as part of your in-depth defense strategy...Tools can help give you comfort and confidence that people are staying within the bounds, but no monitoring tool is going to 100% prevent anything bad or unintended from happening."*
>
> 
>
> Christie Terrill
>
> CISO, Bishop Fox

This is why it's critical to keep humans in the loop when building trustworthy AI governance frameworks. Instead of automatically blocking employee access to AI tools and driving usage outside of the defined business environment (where it's harder to detect), CISOs are increasingly looking for human-centric solutions that address and prevent misuse while helping to deliver effective education and training to employees.

> *Remediation is at its core a behavioral issue: what you need to remediate is the employee. This lies in giving them tools that you do trust. AI tools contain the purest value proposition: using technology to be more productive. When you talk about employee productivity, consider this question: 'How do I change my employees' behavior so they can discover the tools we have vetted, approved, and secured?'"*
>
> 
>
> Russ Spitler
>
> CEO and Co-Founder, Nudge Security

An alternative, hands-on approach that some executives may wish to pursue is governance tools which monitor employees' work outputs for AI usage. This type of AI content detection often involves the use of AI models trained on both human and AI-generated content and using pattern recognition to distinguish between the two. Companies can use these tools to scan and evaluate text, images, audio, and video.

In any case, effective AI Governance strikes a balance between blocking access entirely, sending warnings, making useful tools available via authorized means, and monitoring work outputs for AI-generated content. From a risk management perspective, training and awareness and visibility over model function and employee usage should also be a key element of AI Governance platforms.

3)Tools that identify and target governance for high-impact areas within the organization.

Executives are interested in understanding where AI has a significant business impact (increasing revenue or decreasing costs) and where it may introduce threats to the business. Rather than just having visibility over all the tools employees use for productivity, executive leaders are interested in knowing precisely which tools are involved in business functions that drive a substantial ROI or could pose a threat to their operations.

> *If the business case is great, can be expanded across the organization, and escalate economies by expanding its usage, then the [governance] platform manages those components. The platform should also effectively follow up on the business case, checking whether the investment saves the company X amount of money."*

Hazel Diez Castaño

Global CISO, Santander

Armed with this information, executives can closely monitor data inputs, model performance and behavior, and AI application restrictions based on a clear understanding of risk and reward.

> *Priorities around security have to be around where the biggest economic exposure is, which is loss of client data, loss of intellectual property. For products, there is a different set of risks. On the flip side, there are the efficiency and security benefits that AI brings."*

Evan Wolff

Partner and Co-Chair, Privacy and Cybersecurity Group, Crowell and Moring

For example, the speed of GenAI adoption and the urgency to develop AI applications is also resulting in shortcuts. Models are being rushed into production to keep up with market momentum, leaving security on the back burner. This introduces more vulnerabilities, making vulnerability scanning and pen testing important capabilities to maintain a strong security posture. AI Governance startups with solutions that visualize and address high impact vulnerabilities while linking them to ROI and risk will help their customers make important decisions that align security with business success.

Final Thoughts on the Future of AI Governance

As AI models mature and companies continue to evolve from AI experimentation to material AI and GenAI adoption, the market for AI Governance tools will grow in tandem.

Our take on the market: Bullish

Advanced applications of AI including GenAI bring a wealth of opportunity as well as an expanded attack surface to defend. The growing adoption and development of AI technology necessitates holistic governance. Companies must understand their risk appetites and determine what types of AI governance tools and policies they need based on business value and security priorities. We see high potential for investments in innovative AI governance tools which facilitate discovery, monitoring, detection and response, and data governance going forward.

Here's what could change our minds:

1) If core AI model providers offer self-governance solutions that customers trust and adopt, the market for standalone AI governance entities may not garner much demand.

2) Some CISOs remain apprehensive about whether AI currently introduces enough risk to necessitate governance. In their organizations, governance only takes priority after the budget for AI tools and model deployment is allocated, and dedicated AI governance and risk committees are still being formed. These committees ultimately determine where dollars are spent on AI governance. If these committees remain unformed, it may delay investments in AI Governance tools.

Startups in the AI Governance market have an opportunity to enable safer AI experimentation, integration, and innovation if they can adapt to meet market needs by embracing the key principles of trust and security: business alignment. We look forward to the growth in this space going forward.

Acknowledgements

Special thanks to the following cybersecurity leaders and pioneers for their insights and contributions. If you are a startup interested in meeting with Forgepoint, or would like to be interviewed for future editions of Forgepoint Forward, please contact Rey Kirton at rkirton@forgepointcap.com.

Brian Barrios
VP and CSO, Southern California Edison

Eddie Borrero
CISO, Blue Shield of California

Hazel Diez Castaño
Global CISO, Santander

Elena Kvochko
Adjunct Professor at Cornell University SC Johnson School of Business

Russ Spitler
CEO & Co-Founder, Nudge Security

Christie Terrill
CISO, Bishop Fox

Evan Wolff
Partner and Co-Chair of the Privacy and Cybersecurity Group, Crowell and Moring

Tobias Yergin
Head of Product, Strategic Exploration, Fortune 50 Retailer

Preisha Agarwal
Analyst

Casilda Angulo
Senior Associate

Kathryn Shih
Venture Partner

With the help of Rey Kirton, Conor Higgins, and Tanya Loh

About Forgepoint

Forgepoint is an early-stage venture capital firm that partners with transformative cybersecurity, artificial intelligence, and infrastructure software companies. With the largest sector-focused investment team, over $1 billion in AUM, and an active portfolio of over 30 companies, the firm brings over 100 years of collective company-building expertise and an Advisory Council of nearly 100 industry leaders to support exceptional entrepreneurs. Founded in 2015 and headquartered in the San Francisco Bay Area and London, Forgepoint is proud to cultivate a diverse, global community dedicated to backing builders of the digital future.

Learn more at https://www.forgepointcap.com and https://www.linkedin.com/company/forgepoint-capital.

Company Highlights: AI Governance

BISHOPFOX

Penetration testing and attack surface management

bishopfox.com

nudge

AI, SaaS and cloud account discovery, inventory, and monitoring

nudgesecurity.com

whistic

AI-powered third-party risk management and vendor assessment

whistic.com

Portfolio

Forgepoint is proud to partner with these companies securing the way people live and work. For more information, see https://forgepointcap.com/companies/.

1KOSMOS, aka identity, ANITIAN, AppMap, BISHOPFOX, cinchy, Constella INTELLIGENCE, Converge, CyberCube, FORESCOUT, HUNTRESS, hyperproof, Instabug, interos, loginradius, LUMU, Lynx, NowSecure, nudge, RAD SECURITY, RAFAY, RAPIDFORT, REVERSINGLABS, SECURE CODE WARRIOR, SolCyber, SPHERE, STRATA, SUREFIRE CYBER, SYMMETRY, Synadia, uptycs, VERITUITY, whistic

Exits

CLOUDFLARE AREA 1 SECURITY, Attivo NETWORKS A SentinelOne Company, BehavioSec A LexisNexis Risk Solutions Company, SECUREAUTH | CLOUDENTITY, CYSIV A FORESCOUT COMPANY, ermetic a Tenable company, IDX A ZEROFOX COMPANY, Akamai | noname, Remediant NOW PART OF netwrix, snowflake | truera, concourse A FORTINET COMPANY LABS

Notes

[1] "GenAI Unleashed." Harmonic Security, Jul 29, 2024. www.harmonic.security/resources/genai-unleashed

[2] Mucci, Tim and Stryker, Cole. "What is AI Governance?" IBM, Nov 28, 2023. www.ibm.com/topics/ai-governance

[3] Yépez, Alberto. "How to Conquer the Chaos of SaaS Sprawl and Shadow AI (Nasdaq)." Forgepoint Capital, Aug 6, 2024. www.forgepointcap.com/perspectives/how-to-conquer-the-chaos-of-saas-sprawl-and-shadow-ai/

[4] www.nist.gov/itl/ai-risk-management-framework

[5] www.oecd.org/en/topics/sub-issues/ai-principles.html

[6] digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[7] www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[8] "General Data Protection Regulation (GDPR)," Apr 5, 2016. gdpr-info.eu

[9] Supreme Court's Chevron decision limits tech regulation (axios.com)

Forgepoint

/ Forgepoint Forward /

What's Ahead in AI Governance

Backing builders of the
/digital future/

forgepointcap.com
650.289.4455
400 S. El Camino Real / Suite 1050
San Mateo, CA 94402

Website LinkedIn