Messaging and positioning

AI adoption in your organization is accelerating, but governance isn’t keeping pace. You face hidden risks, regulatory scrutiny, and fragmented oversight. We give you a unified system of record to see what exists, prove compliance, and reduce exposure. The result is faster audit readiness, stronger resilience, and the ability to scale AI with confidence and trust.

With our solutions, you gain clarity across teams, vendors, and infrastructure. You no longer have to rely on scattered reports or manual checks to understand how AI is being deployed. Instead, you have a single view that allows you to connect innovation with accountability and align AI investments with your broader business strategy.

We also shift governance from a defensive task to a competitive advantage. By proving compliance, strengthening resilience, and engaging regulators and partners in shared governance, you build trust inside and outside the enterprise. That trust accelerates adoption, reduces friction with oversight bodies, and positions your organization as a leader in responsible AI at scale.

Benefits

- Gain full visibility into AI projects across teams, vendors, and infrastructure
- Align AI adoption with business strategy and risk management priorities
- Prove compliance with defensible, audit-ready reporting
- Strengthen resilience through continuous testing and remediation
- Enable innovation without increasing enterprise exposure
- Build trust with boards, regulators, customers, and partners

Results

- Faster audit readiness and reduced time spent on compliance prep
- Lower regulatory and reputational risk
- Measurable reduction in vulnerabilities and exposure
- Improved coordination between executives, engineers, and risk leaders
- Higher confidence in scaling AI safely across the business
- Stronger credibility and market differentiation as a responsible AI leader

Messaging and positioning - capabilities

AI adoption is accelerating across every enterprise, but governance has not kept pace. Models are being deployed by different teams, vendors, and business units without clear visibility, consistent controls, or defensible compliance. Leaders face the challenge of enabling innovation while managing risk.

We address this gap with six core capabilities. Each is powerful on its own, but together they create a cycle and a network that transforms AI governance into a managed, scalable business process.

- **Discover** – Expose every model, surface shadow AI, and eliminate blind spots
  Outcome: gain full visibility across the enterprise
- **Inventory** – Map models to data, systems, and vendors to create a single record of truth
  Outcome: align executives, engineers, and risk leaders on one foundation
- **Verify** – Prove compliance with defensible, audit-ready reports
  Outcome: reduce regulatory risk and accelerate audit readiness
- **Test** – Stress models under real threats to reveal vulnerabilities before attackers do
  Outcome: strengthen resilience and build confidence in AI systems
- **Remediate** – Direct fixes through targeted workflows to shrink exposure fast
  Outcome: close gaps quickly and show measurable risk reduction
- **Community** – Share standards across teams, partners, and regulators to build trust
  Outcome: turn governance into credibility and a competitive advantage

Together, these capabilities form both a cycle and a network. They can run end-to-end to complete the governance loop or connect laterally to address urgent needs. This flexibility makes AI governance proactive, responsive, and scalable.

Customer challenges and our capabilities

Traditional data breaches	AI governance failures	Business impact	Our capabilities
Credential theft – stolen usernames/passwords give attackers direct access.	**Shadow AI** – unapproved models deployed without oversight.	Executives lose visibility; AI adoption becomes fragmented and risky.	**Discover** – expose every model, surface shadow AI, eliminate blind spots.
Malware/ransomware – malicious code exfiltrates or locks data.	**Unverified models** – outputs violate regulations or introduce bias.	Regulatory fines, reputational damage, loss of customer trust.	**Verify** – check models against frameworks and produce defensible reports.
Insider threats – employees misuse access to steal or leak information.	**Unvetted vendors** – external models or datasets added without checks.	Vendor risk exposure, supply chain vulnerabilities, accountability gaps.	**Inventory** – map models to data, systems, and vendors in a single record.
Database/server exploits – attackers exploit misconfigurations or vulnerabilities.	**Untested resilience** – models fail under stress or adversarial attacks.	Operational disruption, compromised decisions, security breaches.	**Test** – stress models under real-world threats and adversarial conditions.
Third-party/vendor breaches – partners compromised to reach data.	**Compliance breakdowns** – no audit-ready proof, triggering penalties.	Audit failures, legal risk, and loss of market credibility.	**Remediate + Community** – close gaps with targeted fixes, share standards, and build trust.

Traditional security protects data. We govern AI systems by exposing shadow projects, proving compliance, testing resilience, and helping enterprises avoid penalties, reputational damage, and loss of trust.

Messaging matrix by persona and capability

	Discover	Inventory	Verify	Test	Remediate	Community
CIO	Gain visibility into all AI projects to eliminate hidden risk.	See a complete record of AI assets to align investments with strategy.	Demonstrate compliance posture with defensible reports.	Understand resilience gaps without technical deep dives.	Ensure teams fix issues quickly to stay on track.	Share governance practices to build trust in enterprise AI.
CISO	Detect unapproved AI use and eliminate blind spots.	Know which models and vendors are in scope for risk management.	Validate AI systems against security frameworks.	Simulate adversarial attacks to find vulnerabilities first.	Apply security controls that reduce exposure at scale.	Collaborate with regulators and partners on AI security.
CTO	Map all models in use for architectural oversight.	Maintain a living record integrated into MLOps and DevOps.	Track governance readiness across deployed models.	Confirm model resilience under load and stress.	Embed remediation workflows into engineering pipelines.	Align teams and vendors under shared governance.
Data Science Leader	Discover models across teams to avoid duplication.	Document lineage of models and data for reproducibility.	Prove compliance checks before release.	Catch bias and vulnerabilities early with testing.	Get actionable fixes to speed approvals.	Share benchmarks with peers to improve model quality.
Security Analyst	Spot hidden or unauthorized AI systems.	Access inventories for faster audits and investigations.	Automate compliance evidence gathering.	Run real-world tests to generate actionable alerts.	Receive prioritized remediation tickets.	Coordinate with analysts and compliance teams.
Risk & Compliance Officer	See the full scope of AI systems under governance.	Build a defensible audit trail of models and vendors.	Automate attestations and audit-ready reports.	Validate readiness of high-risk models.	Ensure corrective actions are logged for audit purposes.	Engage peers, partners, and regulators in transparent governance.

Themes and topics

Top 5 SEO keywords

- ai governance platform
- enterprise ai governance
- ai risk management
- ai compliance software
- ai audit readiness

Top 5 GEO keywords

- what is ai governance and why does it matter
- how do enterprises manage ai risk
- how to comply with ai regulations
- how to test ai models for security and resilience
- what are the risks of shadow ai in business

The AI governance gap

- AI adoption is outpacing oversight
- Why enterprises lack visibility and controls
- The cost of inaction

From policy to proof

- Moving beyond compliance statements
- Defensible, audit-ready evidence for boards and regulators

Shadow AI risk

- Hidden models deployed outside oversight
- Business and regulatory exposure

AI as a system of record

- Why enterprises need a unified inventory of models, data, vendors
- Turning scattered projects into a managed foundation

AI resilience

- Testing and stress conditions
- Preparing for real-world adversarial threats

Operationalizing governance

- Governance as a repeatable business process, not a one-off exercise
- Scaling across roles, teams, and vendors

Innovation with guardrails

- How governance enables safe AI adoption
- Balancing innovation speed with accountability

Trust as a competitive advantage

- Turning compliance into credibility in the market
- Differentiating with transparency and shared standards

Regulatory readiness

- Global AI regulation landscape
- Preparing for evolving frameworks (NIST, EU AI Act, etc.)

Foundational content BOM

- **Corporate solution brief:** One-pager that explains our AI platform, overarching value, and business outcomes
- **Executive overview deck:** Pitch deck that tells the full story: market challenge, platform value, six capabilities, results, and proof points
- **Thought leadership report (hero asset):** Analyst brief or white paper: *The State of AI Governance 2026*. Positions us as the voice of authority.
- **ROI calculator and business case tool:** Interactive or static model that shows how solutions reduce risk, save time, and accelerate audit readiness
- **Customer story library:** 3-5 multi-format customer stories (written + video) highlighting enterprise impact across industries.
- **Demo video (platform-level):** Walkthrough of our full governance loop, not just individual capabilities
- **Messaging and positioning framework:** Internal guide aligning value props, messages, proof points, and differentiators across personas
- **Competitive positioning sheet:** Battlecard or comparison doc showing how our solutions differ and beat out the competition

Content BOM for each capability

Each capability is complex on its own, but customers, partners, and sales teams **need clarity, proof, and a path to action**. By **standardizing main content types across all six capabilities**, we create a modular toolkit as a starting point to **drive our content engine:**

- **Mini MPF and narrative**– internal guide with value prop, key messages, proof points, and personas
- **Pitch deck** – sales-ready slides tailored to the capability, highlighting business value, proof, and visuals
- **Solution brief** – concise overview of the capability, problem solved, and business outcomes
- **Hero and supporting assets** – hero asset (gated white paper, analyst report, ebook, interactive content) establishing authority and urgency, with supporting assets to promote (infographic, social carousel)
- **Demo video** – short walkthrough showing the capability in action
- **Blog post** – top-of-funnel content introducing the challenge and solution
- **Customer story** – narrative showing the customer’s journey and impact

Quarterly content calendar per capability

Category	Hero Asset	Funnel	Trigger	Supporting Assets	Adoption / Retention Asset
Discover	White paper: The Hidden Risk of Shadow AI	Awareness	CIO/CISO realizes AI tools are used outside IT oversight	1 blog, 1 infographic, 1 webinar, 1 sales brief	Product tutorial
Inventory	Case study: Cutting Audit Prep Time in Half	Decision	Compliance team overwhelmed by audit prep	1 blog, 1 solution brief, 1 social carousel, 1 analyst blog	Onboarding guide
Verify	Analyst report: The State of AI Compliance 2025	Awareness	New regulation or board compliance concerns	1 blog, 1 webinar, sales brief, 1 infographic	Compliance playbook
Test	Interactive guide: Red-Teaming AI	Consideration	Teams prepping models for production	1 blog, 1 video demo, 1 social series, 1 technical brief	Workshop
Remediate	Customer success story: Cutting Time-to-Fix from Weeks to Days	Decision	Security/compliance leaders want proof of faster remediation outcomes	1 blog, 1 demo, 1 infographic, 1 ebook excerpt	Customer success webinar
Community	Roundtable webinar: Building Trust in AI	Consideration	Regulators or partners call for transparency	1 blog, 1 social explainer, 1 partner story, 1 analyst Q&A	Customer council