



Unlocking the Power of AI

**Driving Business Growth
While managing Data Security
and Privacy Risks**

Table Of Contents

Executive Summary

- 01** AI Adoption: Current and Forecasted
- 02** AI Drives Efficiency and Innovation
- 03** Barriers to AI Adoption: Data Privacy and Skills
- 04** The Key Risks of Using AI
- 05** Conclusions

Appendix: Survey Demographics

Executive Summary

Unlocking the Power of AI: Driving Business Growth While Managing Data Security and Privacy Risks is a report derived from a survey we conducted on AI usage in business. It explores Artificial Intelligence's (AI) role in enhancing efficiency, and growth while addressing critical data security & privacy challenges. As AI adoption increases, organizations must balance the substantial benefits with notable risks, necessitating a strategy that delivers business value while mitigating risks.

Key Takeaways

- 93.8%: Organizations currently using or planning implement AI within the next six months
- 83.8%: Organizations reporting significant or moderate improvements in business operations through AI use.
- 72%: Respondents who identified data exposure as the top risk in AI deployments.

Key Findings

AI adoption is widespread and expected to grow, with 90.6% of surveyed organizations currently using or planning to implement AI in the next six months. This expansion reflects AI's perceived value in boosting operational efficiency and supporting innovation. Survey results show that 83.8% of respondents report significant or moderate improvements in operations, with 64% citing increased efficiency and 56% highlighting AI's role in innovation and product development. However, rapid AI integration also poses challenges, with high costs, legacy system compatibility, and data privacy concerns being primary barriers. AI's reliance on extensive datasets increases risks such as data exposure, data theft, and consent violations, with 72% of respondents citing data exposure as a top AI risk. Effective risk management demands collaboration among Security Architecture, Security Operations, Privacy, and Compliance teams to create secure, responsible AI implementations.

Recommendations

Conduct Routine AI Risk and Privacy Assessments:

Regular assessments involving cross-functional teams can help identify vulnerabilities and strengthen data privacy measures.

Implement Strong Data Security Controls:

Establishing layered controls, such as classification and access restrictions, helps safeguard sensitive data and prevent unauthorized access.

Establish Clear AI Governance Policies:

Develop governance policies covering data consent, usage, and auditing requirements to ensure transparency and accountability.

These strategies enable organizations to harness AI's transformative potential while protecting data integrity, fostering growth and trust.

AI Adoption: Current and Forecasted

Key Takeaways

- 85.8% of organizations already use AI for at least one project.
- 93.8% are either currently using AI or planning to in the next 6 months.
- 66.2% of organizations are using third-party AI solutions for at least some of their AI projects.

The survey revealed that 93.8% of respondents are either using or planning to use AI in the next 6 months. The diversity in adoption spans multiple departments, reflecting the growing recognition of AI's potential in improving efficiency and driving innovation. However, adopting AI without adequate governance exposes organizations to significant security and privacy risks, including unauthorized access to sensitive data, unintentional biases in decision-making, and potential regulatory non-compliance, all of which can lead to reputational damage, legal consequences, and financial losses.

This demonstrates the cross-functional applicability of AI within organizations and its strategic importance to drive business growth.

This chart illustrates that AI projects are widespread, with 85.8% of respondents either using AI or under active implementation.

How would you characterize AI usage within your organization?



14.2%: Under active investigation

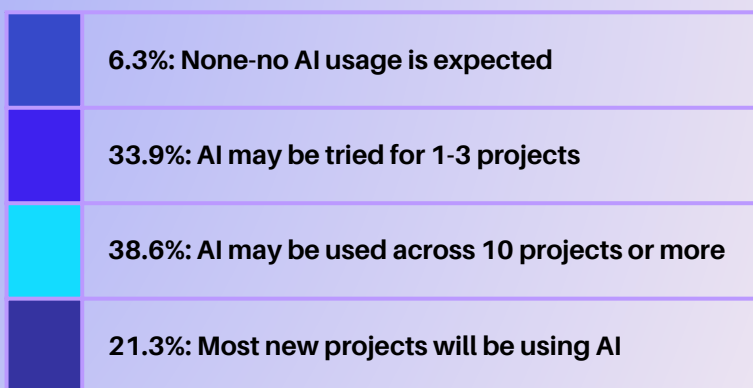
25.2%: Under active implementation

30.7%: Already using AI for one project

29.9%: Already using AI across multiple projects

This chart illustrates that AI projects are widespread, with over 93.8% of respondents either using AI or planning future implementations.

In the next 6 months, what do you forecast to be the state of AI usage within your organization?



This chart shows that 66.2% of organizations are using third-party AI solutions or a combination of in-house and third-party solutions.

Are you using third-party AI solutions or developing in-house AI tools?



Recommendations

- **Adopt a Risk-Based Approach to Data Governance:**

Conduct regular AI risk assessments and privacy impact assessments focusing on data sensitivity and compliance requirements. This involves creating a data governance framework that classifies data by risk level and outlines specific security measures, access controls, and audit requirements for each classification to minimize privacy risks.

- **Implement Privacy-Enhancing AI Technologies:**

Invest in privacy-preserving techniques such as federated learning, data minimization, and encryption methods that allow data to be used for AI training without exposing sensitive information. This approach ensures data privacy while unlocking AI-driven insights for business growth.

- **Establish Transparent AI Policies and Communication Channels:**

Develop clear policies regarding data usage, AI use and modeling decisions, and privacy practices. Regularly communicate these policies to employees and customers and include them as part of employee training requirements, promoting trust and accountability. Transparency around AI use can strengthen stakeholder confidence, facilitating broader AI adoption while addressing privacy concerns effectively.

- **Ensure Data Sovereignty with Third-Party AI Solutions:**

Before integrating third-party AI solutions, verify that vendors maintain strict data sovereignty controls, allowing you to retain ownership and control over sensitive data used in model training. This helps prevent data exposure, ensures compliance with regional regulations, and mitigates the risks associated with data sharing across borders.

AI Drives Efficiency and Innovation

Key Takeaways

- 83.8% of respondents significantly or moderately improved business operations by using AI
- 64% of respondents identified increased efficiency as the primary benefit of AI adoption.
- 56% highlighted innovation and product development as a key benefit of implementing AI
- 90.6% believe that AI will play a critical role in future business growth.

Adopting AI offers businesses substantial operational and strategic advantages, as confirmed by survey findings where 83.8% of respondents reported significant or moderate improvements in business operations through the use of AI. Increased efficiency was a primary benefit for 64% of respondents, with AI optimizing processes and streamlining workflows traditionally reliant on more time and resources. Moreover, 56% noted AI's role in driving innovation and product development, enabling companies to stay competitive by enhancing existing products and creating new offerings. Importantly, 90.6% believe AI will play a critical role in future business growth, underscoring AI's position as a powerful engine for productivity, innovation, and market leadership.

The chart shows the reported impact on business operations, with 83.8% of respondents showing significantly or moderately improved business performance from AI.

How has AI impacted your business operations so far?



8.7% Negative impact

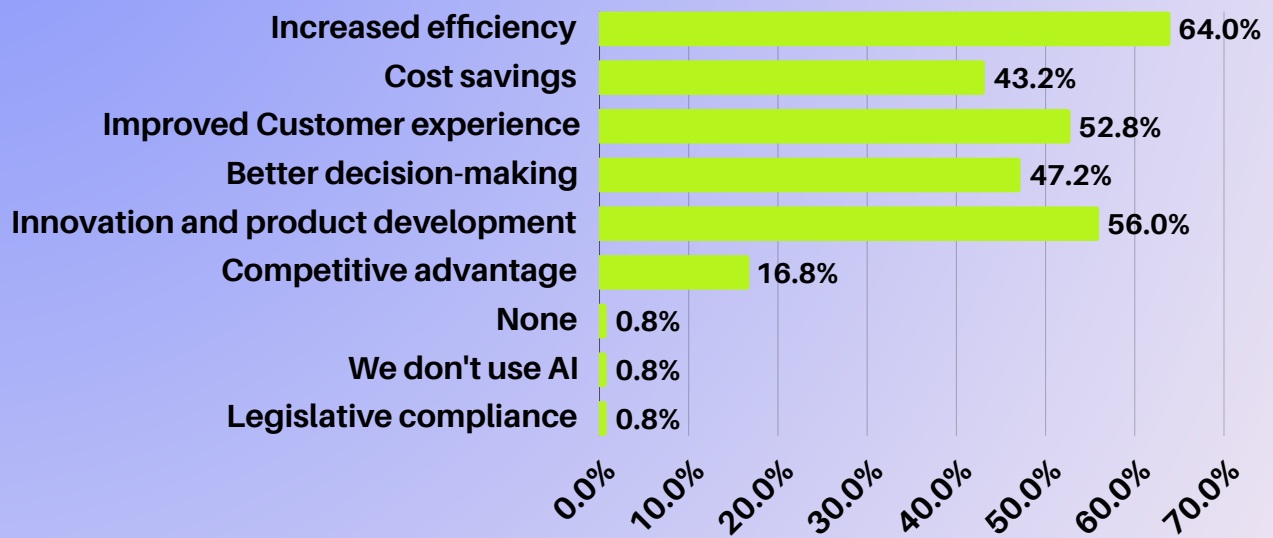
42.7%: Significantly improved

41.1%: Moderately improved

13.7%: No significant impact yet

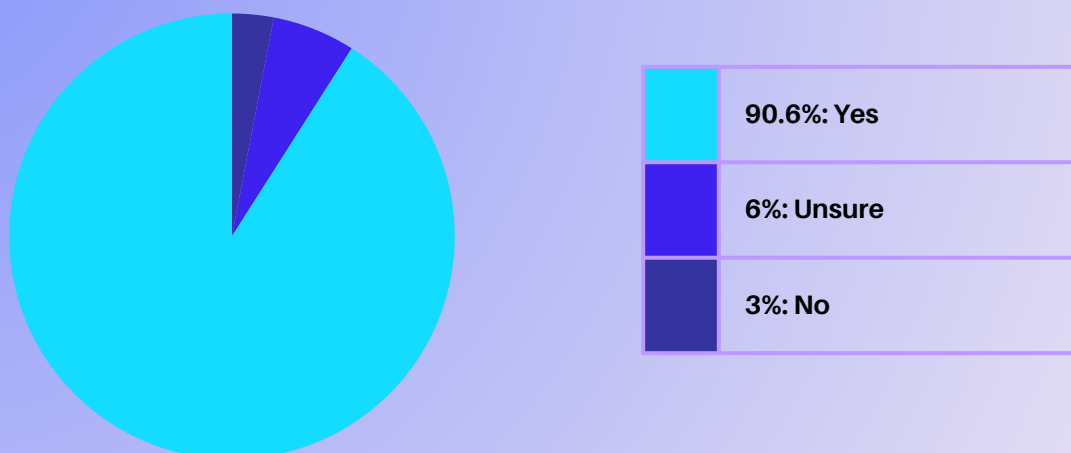
The chart shows the top benefits reported by respondents, underscoring the broad applicability of AI across departments for improving efficiency, customer service, and cost reduction.

What are the primary benefits you've observed from using AI in your business?



90.6% of respondents believe AI will play a critical role in their business's future growth.

Do you believe AI will play a critical role in your business's future growth



Recommendations

- **Align AI Initiatives with Business Goals and Customer Needs:**

Design AI projects to directly address specific business objectives, such as improving customer experiences, reducing operational costs, or creating product innovations. By aligning AI applications with strategic goals and customer insights, businesses can maximize their impact and relevance.

- **Prioritize Data Security and Privacy in AI Deployments:**

Implement robust security measures, such as encryption and access controls, and utilize privacy-enhancing methods like data minimization to protect sensitive data. This approach not only mitigates privacy risks but also fosters trust among customers and stakeholders.

- **Continuously Monitor and Improve AI Models:**

Regularly evaluate AI models for accuracy, relevance, bias, and compliance with privacy standards. Continuous improvement, along with routine updates based on new data, allows businesses to maintain AI's effectiveness and security over time, sustaining efficiency gains and innovation efforts.

Key Takwways

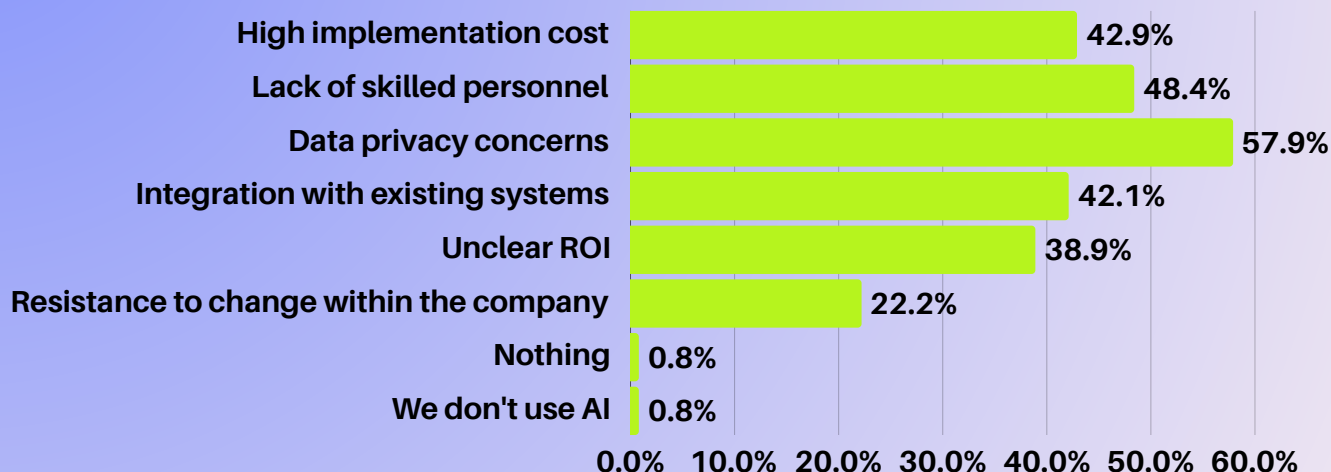
- High implementation costs, integration with legacy systems, and data privacy concerns were cited as the primary barriers to AI adoption.

Barriers to AI Adoption: Data Privacy and Governance Skills

Despite AI's advantages, organizations encounter significant challenges in its implementation, particularly around data privacy and talent shortages. According to the survey, high costs, integration with legacy systems, and data privacy issues stand out as primary barriers to AI adoption, affecting teams across Security Operations, IT, and Privacy. As AI becomes more embedded in business functions, security and privacy teams are increasingly tasked with ensuring data integrity and compliance, navigating complex regulatory landscapes to mitigate risks associated with sensitive data use. Additionally, the lack of skilled personnel is a critical hurdle, as organizations struggle to find experts who can develop, deploy, and maintain AI systems while upholding stringent security standards. These challenges highlight the need for targeted investment in both talent and technology to maximize AI's potential while safeguarding data privacy.

This chart reflects the primary concerns businesses face when integrating AI into their operations, particularly related to cost and privacy risks.

What challenges have you faced in implementing AI?



Recommendations

- **Invest in Specialized Training and Upskilling Programs:**

Develop in-house training and certification programs to enhance employees' AI skills, focusing on data privacy, security protocols, and ethical AI practices. Upskilling existing staff can help fill critical roles and reduce dependency on external hires.

- **Establish Cross-Functional Privacy and Security Protocols:**

Create a collaborative privacy by design framework between Security Operations, Privacy, and IT teams to address data privacy and compliance issues from the start of AI projects. This ensures that AI systems are designed with security and privacy in mind, minimizing risks as they integrate across departments.

- **Implement AI Governance Policies and Data Security Controls:**

Establish comprehensive governance policies and data security controls to monitor and manage the use of sensitive data in AI projects. Regular audits, access controls, and compliance checks should be integrated into AI workflows to ensure data privacy, regulatory adherence, and secure AI deployment across the organization.

The Key Risks of Using AI

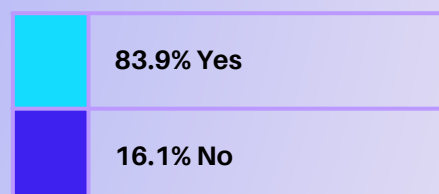
Key Takeaways

- The responsibility for ensuring AI governance and security is spread across multiple teams including Security Architecture, Security Operations, Privacy, and Compliance.
- 83.9% of respondents have conducted an AI risk assessment.
- 72% cited Data Exposure at the top risk for AI deployments.

Deploying AI presents several key risks, particularly in terms of data exposure, data theft, and consent violations. As AI models rely heavily on vast datasets, they may inadvertently expose sensitive information if proper safeguards aren't in place. This risk extends to data theft, as hackers target AI systems to gain access to confidential data used in training and decision-making processes. Additionally, AI deployments can easily overlook consent requirements, leading to unauthorized use of personal data that violates privacy regulations. To mitigate these risks, it's essential for security architecture, security operations, privacy, and compliance teams to collaborate. By working together, they can implement robust security frameworks, enforce stringent access controls, and conduct regular compliance checks to ensure that AI initiatives uphold data protection standards and operate within regulatory guidelines. This cross-functional approach is crucial to building a secure, responsible AI environment that minimizes exposure and maintains trust.

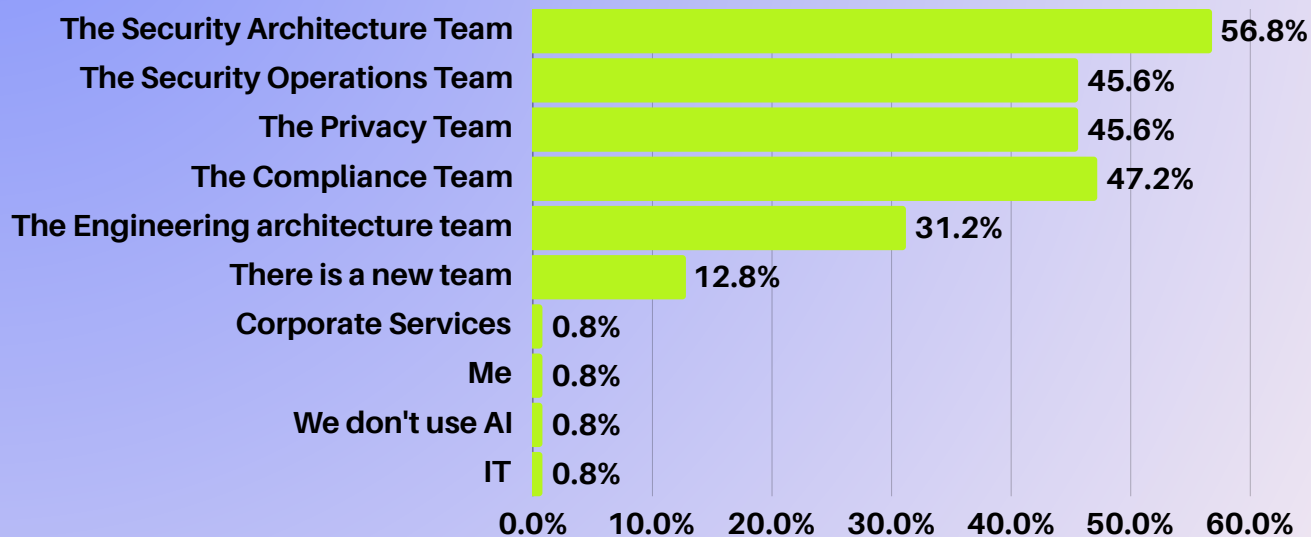
An overwhelming majority of respondents completed a risk assessment of their AI use.

Have you completed a risk assessment of your use of AI?



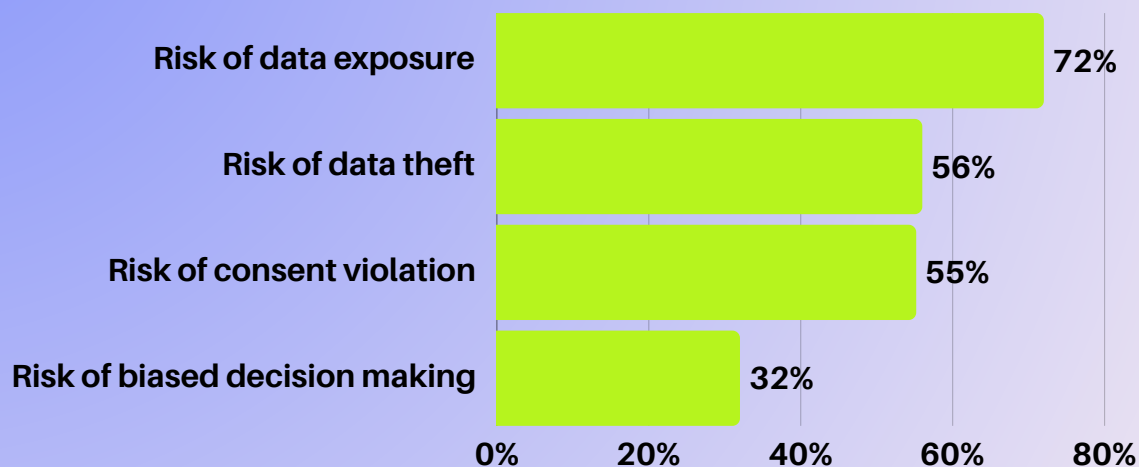
This chart shows which departments are most often responsible for AI Governance and Security.

Which department(s) within your organization are responsible for ensuring AI governance and/or AI security?



The top three risks cited by respondents were data exposure, data theft, and consent violations.

What would you characterize as the greatest risks associated with using AI for your business?



Recommendations

- **Conduct Comprehensive AI Risk and Privacy Impact Assessments (PIAs) to Prioritize Data Exposure Mitigation:**

With 72% of respondents identifying data exposure as the top risk, regularly perform both AI risk assessments and privacy impact assessments (PIAs) to proactively identify vulnerabilities and safeguard sensitive information. These evaluations should be cross-functional, engaging Security Architecture, Privacy, and Compliance teams to ensure a holistic approach to risk and privacy management. Together, these assessments help mitigate exposure risks and strengthen the organization's AI governance framework.

- **Implement Layered Data Security Controls and Access Restrictions:**

Develop a robust security framework that includes layered data protection, encryption, and access controls to minimize unauthorized access and potential data theft. Security Operations should lead efforts to monitor AI data flows and implement stringent access management, ensuring that sensitive data is only accessible by authorized personnel.

- **Enforce Strict Consent Management and Compliance Protocols:**

To prevent consent violations, establish policies that require clear, documented consent for all data used in AI models, with regular compliance checks to verify adherence. Privacy and Compliance teams should work together to monitor AI data usage and maintain a clear audit trail, ensuring AI practices align with privacy regulations and customer expectations

Conclusion

Using AI to Drive Growth While Mitigating Business Risks

As AI adoption reshapes business landscapes, its potential to drive efficiency, innovation, and growth is increasingly clear. This report emphasizes that while organizations are eager to leverage AI, they must carefully address challenges around data security, privacy, and regulatory compliance. Implementing strong governance policies, robust data security protocols, and routine privacy impact assessments (PIAs) and AI risk assessments will help protect sensitive information and ensure regulatory compliance. PIAs, in particular, are essential for evaluating potential privacy risks early in AI projects, allowing organizations to identify and mitigate issues around data exposure, theft, and consent violations.

Collaboration across Security Architecture, Security Operations, Privacy, and Compliance teams will be instrumental in building a secure and responsible AI framework. These cross-functional efforts ensure that AI systems are not only innovative but also align with privacy and security standards, fostering trust among customers and stakeholders. Ultimately, balancing innovation with responsible data management, backed by regular PIAs, is essential for sustaining AI-driven growth and positioning organizations as leaders in a data-centric future.

About LightBeam

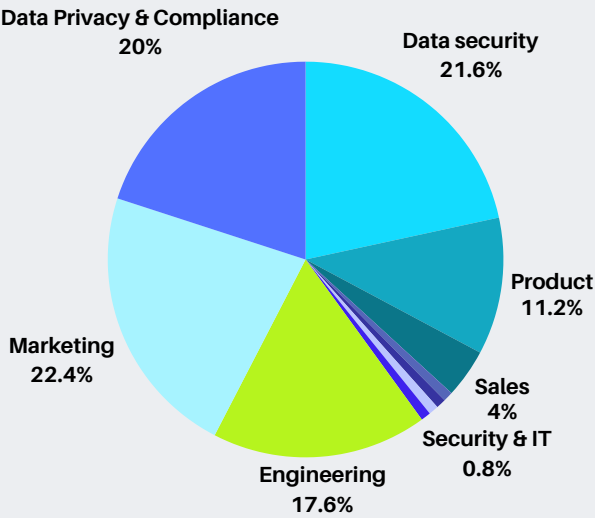
LightBeam is an Identity-centric data security solution that reduces breach risks, ransomware costs, and regulatory penalties by integrating data security posture management (DSPM), privacy, and governance into a single converged platform. Powered by patented Data Identity Graph technology, LightBeam uses AI to discover and map sensitive data across both structured and unstructured data sources including shadow data to determine the business context and human identity information. This unique understanding of data identity enables LightBeam to instantly customize data governance policies, automate complex and manual privacy tasks (DSR, RoPA, Consent), and more accurately protect sensitive data through redaction and anonymization.

Appendix:

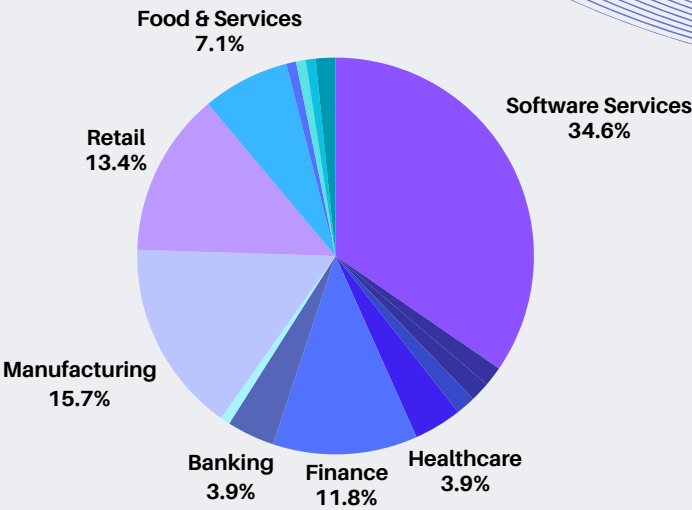
Survey Demographics

Survey data was collected in the fourth quarter of 2024. Here are the demographics of the 127 respondents:

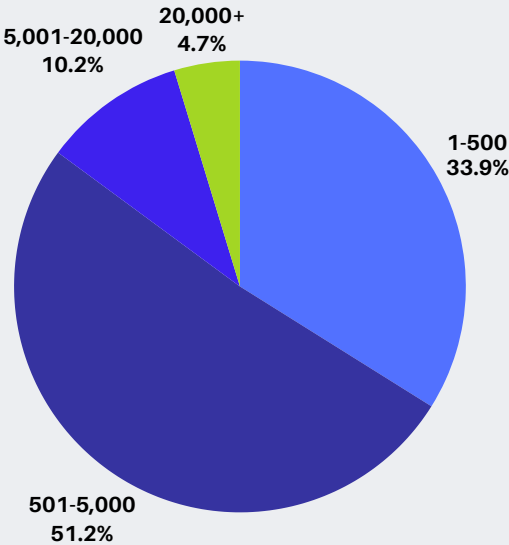
Role in company



What industry does your business operate in?



How many employees does your business have?





www.lightbeam.ai

LightBeam.ai , Inc., Palo Alto, CA, USA
+1 (650) 224 8706 | sales@lightbeam.ai