



451 Research Market Insight Report Reprint

Coverage Initiation: LightBeam.ai aims to illuminate gaps in enterprise data security, governance and privacy

April 23, 2024

by **Paige Bartley**

Data governance and privacy practices not only support compliance, they are critical to ensure the ready flow of usable data throughout the organization. LightBeam.ai has adopted a platform-based, zero-trust approach toward discovering, securing and democratizing data sources, handling privacy and security requirements along the way.

S&P Global
Market Intelligence

This report, licensed to Lightbeam.ai, developed and as provided by S&P Global Market Intelligence (S&P), was published as part of S&P's syndicated market insight subscription service. It shall be owned in its entirety by S&P. This report is solely intended for use by the recipient and may not be reproduced or re-posted, in whole or in part, by the recipient without express permission from S&P.

Introduction

LightBeam.ai is seeking to help organizations find any gaps they might have in their data governance and privacy programs by adopting a zero-trust and converged platform approach for data discovery, cataloging, control and compliance — across all data sources, from structured to unstructured. The company intends to help customers unify their siloed data governance and privacy strategies for the purposes of business acceleration and compliance.

THE TAKE

One of the biggest challenges in enterprise data governance and privacy efforts is the coordination of relevant stakeholders and their duties. There are many parties involved in these initiatives, and they often adopt (or prefer) certain point tools for specific steps in the data governance and privacy workflow. This can lead to technological fragmentation — paradoxically, making the control of sensitive enterprise data more difficult. With its architecture for data security, governance and privacy, LightBeam.ai is looking to unify the software layer for these tasks so that there is less need to integrate unwieldy, competing tools.

The vendor's broader ambition is not simply to help organizations achieve compliance, although it helps to facilitate that objective. Its ultimate goal is to provide consistent visibility, documentation and stewardship of business data resources so that these data types can be safely used for analysis, AI/ machine learning and insight while balancing controls for privacy. However, LightBeam.ai could face headwinds in finding a consistent purchase influencer or “champion” within prospect accounts. Given that its product spans a broad range of data security, governance and privacy functionality, identifying the most relevant stakeholders within any given organization could be a challenge.

Context

The layperson's interpretation of enterprise data governance and privacy efforts is frequently married to the concept of regulatory compliance, yet companies today want to achieve much more in their initiatives. According to 451 Research's Voice of the Enterprise: Data & Analytics, Data Governance & Privacy 2024 survey, the top-reported business outcomes motivating organizations to improve data governance functionality are higher quality of data/insight (43.5%), faster access to relevant data (38.8%) and enhanced AI/ML outcomes (29.4%). Security and privacy requirements are still pressing and relevant, yet organizations are looking to turn those needs in their favor and accelerate other business outcomes via better visibility and control of data resources.

LightBeam.ai was launched in 2020, largely pulling its key talent and leadership from multicloud architecture specialist Nutanix Inc. Co-founder and current CEO Himanshu Shukla was formerly the head of AIOps at Nutanix, and fellow co-founder and Chief Product Officer Priyadarshi Prasad also came from Nutanix. Co-founder Aditya Ramesh, the company's chief architect, shares a similar professional heritage, formerly holding the title of senior architect for Nutanix Compute.

The company originated based on the data governance and privacy workflow needs (as well as complications) that arose while its founders were at Nutanix. During the early era of the General Data Protection Regulation enforcement circa 2018-2019, the founders — while at Nutanix — participated in workflows to support customer requests to manage (and sometimes, delete) data.

Although Nutanix was classified as a data processor under GDPR and had shared responsibilities with its data controllers to manage and protect personal data, LightBeam.ai's founders ascertained that unified visibility and control of this data was largely manual and often insufficient. They set out to create a technological approach that would stitch together this necessary view amid fragmented software tools, providing mechanisms to remediate or adequately protect sensitive data resources so that they can meet compliance requirements while still being deployed in proactive initiatives such as analytics, AI/ML and data self-service.

LightBeam.ai is based in Palo Alto, Calif., with offices in other locations throughout the US, Canada, Germany and India. The vendor has roughly 100 employees. It has raised \$22 million in funding, with the most recent capital infusion coming from a \$17.8 series A round in February that was led by new investor Vertex Ventures US and included participation from Dropbox Ventures, as well as existing backers 8VC, Village Global Management and several angel investors.

Products

The company's flagship platform features integrated capabilities for data security, privacy and governance. The foundation of the platform's functionality is based on privacy-aware data discovery capabilities, including tools for identity resolution to enable sanctioned users within the organization to not only find sensitive data, but also pinpoint what person or customer that data is associated with. By discovering and cataloging sensitive data types — structured, semi-structured and unstructured — across hybrid IT architecture, the platform helps organizations assess and define their risk footprint as it relates to internal data sources.

However, simply defining and assessing data-related risk is typically just a starting point for any organization concerned about meeting compliance requirements or accelerating their data-driven activities. The business needs to be able to remediate risky settings for datasets, protect sensitive data in a continuous but dynamic fashion, and ensure ongoing visibility into the data stack.

This is where LightBeam.ai's data governance and data privacy controls come into play. Its platform provides cataloging for SQL and NoSQL data sources; can discover sensitive data in SaaS applications, including unstructured file shares; and has document classification functionality supported by active learning techniques that allow the organization to classify information based on specific business needs. Sensitive content can be secured via a variety of controls, including redaction of sensitive text/fields and anonymization techniques so that data can still be utilized for analysis and insight.

The platform's Privacy Center offers organizations a customer- or consumer-facing portal where individuals can access self-service tools for requesting their personal data (e.g., data subject access requests), as well as manage settings for cookie consent and consent management. This portal, integrated with the rest of LightBeam.ai's platform, leverages extensive automation to retrieve relevant customer/consumer data when and where it is needed, under the right conditions, as well as propagate reported preference settings to the personal data already existing in the enterprise data ecosystem.

According to our survey cited earlier, nearly one-fifth (18.1%) of respondents report that "number of customer/consumer rights requests" is a top technical challenge in managing data privacy within the organization, and another 28.5% report that "lack of automation" is a challenge. With its Privacy Center, LightBeam.ai is aiming to address both privacy pain points.

In building its platform, the vendor was seeking to help organizations streamline data security, governance and privacy architecture that — in many cases — had previously been fragmented by numerous individual tools. The platform's combination of broad sensitive data discovery capabilities combined with controls for data protection and privacy — along with a data subject-facing portal for fulfilling rights requests and preferences — unifies the technologies and workflows for these interrelated business functions. Additionally, LightBeam.ai provides a Privacy at Partners portal for understanding what data is leaving the organization to third parties — and how.

The vendor's platform leverages zero-trust architecture in which it is deployed either on-premises or in the customer's private cloud environment. Because of this design, there is no exfiltration of sensitive enterprise data from the client's IT ecosystem, and no external access to the organization's data sources. No enterprise data or metadata ever has to leave the customer's infrastructure or network.

Strategy

LightBeam.ai is focused on taking its platform to market primarily with medium-sized and large enterprise customers — organizations that have sufficient IT complexity and relatively high volumes of potentially sensitive data. While the company has made strides to move upmarket recently, midsize enterprises — which we generally define as having 100-1,000 employees — still form a significant proportion of its client base. Midsize enterprises often face the most difficulty in managing data governance and privacy requirements; while they have the same data-driven regulatory requirements as their larger industry peers, they frequently lack the internal staffing and resources to manually configure and maintain settings to protect and steward this information in a highly consistent way.

For product licensing, LightBeam.ai employs a mix of models depending on the customer's existing IT environment and architecture that will connect to the platform. For mainstream applications that have direct connectivity to LightBeam.ai, pricing is partially determined on the number of seats. For all other apps, the vendor utilizes connector-based pricing. The rationale behind this approach is that it keeps the barrier to entry low for clients and offers relative predictability of associated costs. For a few very large enterprise customers, the company has already experimented with consumption-based pricing (enterprise licensing agreements), although this is more of a bespoke model.

Competition

LightBeam.ai's most relevant competition likely comes from other data governance and privacy-oriented providers that deploy sensitive data discovery and classification as the main basis of their technical stacks. Some of the names in this arena include 1touch.io, Ardent Privacy, BigID, Concentric.ai, DataGrail, Ethyca, Fasoo, Mine, Privado, Relyance AI, Securiti, Secuvy and Transcend. However, BigID and Securiti are LightBeam.ai's most relevant rivals in the enterprise sales cycle.

Other large software suppliers have sensitive data discovery and classification capabilities, often paired with modules or functionality for data security, privacy and governance. All of the US-based cloud hyperscalers — AWS, Google and Microsoft Corp. (Azure) — have some sort of tooling available to address these needs. Microsoft pairs its AI-driven Security Copilot with its Purview functionality for data governance. Informatica Inc. is another incumbent in the data management space that has AI-driven features for protection and management of sensitive data, primarily via its acquisition of Privitar in 2023.

PrivacyOps specialists have long been trying to unify and streamline unwieldy enterprise data privacy workflows. One of the major players in this space is OneTrust, whose pickup of Integris Software in 2020 brought it a data discovery layer to complement its existing privacy management and consent/preference features. TrustArc also vies in this arena. Other smaller PrivacyOps specialists include 2B Advice, DPOrganizer, Ketch and Osano. Additionally, CYTRIO offers a consolidated platform for data privacy management.

The data security posture management space, which also generally seeks to identify and map sensitive data sources, is increasingly bleeding across market boundaries into the data governance and privacy sectors. Some of the DSPM specialists that might be relevant here include CrowdStrike (Flow Security), DoControl, Normalyze, Palo Alto Networks Inc. (Dig Security) and Rubrik (Laminar). Others that have a stake in this sector include major incumbents such as IBM Corp. and Varonis Systems Inc., as well as midsize players like Netwrix (with its acquired Stealthbits assets).

SWOT Analysis

<p>STRENGTHS</p> <p>LightBeam.ai has a vision to unify and coordinate multiple interdependent functions within the organization via a streamlined stack that minimizes data silos. When implemented and connected appropriately, its platform can theoretically replace up to three or more fragmented products for data security, privacy and governance use cases. This unified approach can help coordinate the activities of multiple stakeholder groups.</p>	<p>WEAKNESSES</p> <p>The vendor is a relatively young and small entrant in a buzzy corner of the space. The breadth of its platform is a strength, but this scope of functionality means that there could be multiple enterprise stakeholders that need to be swayed in a sales cycle, and that there might be buyer concerns about lock-in. LightBeam.ai will likely need to hone its target persona and associated messaging, especially as it moves upmarket.</p>
<p>OPPORTUNITIES</p> <p>Data privacy and governance are becoming more interdisciplinary practices. With its easy-to-use and automated features, LightBeam.ai's converged platform approach could appeal to the growing audience of data governance and privacy stakeholders that previously might have been excluded from more technical aspects of workflows due to a lack of training or specific skills.</p>	<p>THREATS</p> <p>Sensitive data discovery and classification, in particular, is not a new concept — many incumbents have offerings that they can pair with other privacy- and governance-oriented products and services. While LightBeam.ai touts the unified and zero-trust architecture of its platform, potential customers could gravitate toward the perceived credentials and flashier marketing efforts of larger software providers.</p>

CONTACTS

Americas: +1 800 447 2273

Japan: +81 3 6262 1887

Asia-Pacific: +60 4 291 3600

Europe, Middle East, Africa: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence

www.spglobal.com/en/enterprise/about/contact-us.html

Copyright © 2024 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global keeps certain activities of its divisions separate from each other to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain nonpublic information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.