REPORT REPRINT

Coverage Initiation: Concentric's data access governance leverages semantic awareness of risk

DECEMBER 11 2020

By Paige Bartley

Making sure the right people have access to the right data, at the right time, has grown more complicated with expanded remote work and high volumes of unstructured data. Concentric, with its semantic and autonomous approach to data access governance, looks to identify and protect data in a thematic way based on relative risk.

451 Research

S&P Global
Market Intelligence

Introduction

Unstructured data types – especially those that are based on natural language – are typically the workhorse of day-to-day communication and collaboration within the enterprise. Few can imagine a functioning business environment without text documents or PDFs. Yet as data privacy and protection regulations around the world become more stringent and nuanced, there is a business imperative to protect the potentially sensitive data that exists within these unstructured data sources. Traditional approaches have often relied on the participation of content creators, who may inadvertently move sensitive content from a secure location to an unsecure one. These approaches also often depend on restricting access to certain documents, folders or data sources based on rules relating to simplistic employee characteristics, such as current role. In doing so, rough categories are created, and friction arises with employee access to data, slowing down workers.

Today's expanded remote work reality has emphasized the importance of seamless, yet appropriate, worker access to unstructured data. In 451 Research's Voice of the Enterprise: Workforce Productivity & Collaboration, Work Execution Goals & Challenges 2020 survey, participants reported that their number one obstacle to collaborative team success was that 'information is siloed in different applications, making it difficult to search, access and use,' with 25% of participants reporting this challenge. Concentric's approach to data access governance for unstructured data looks to refine the access-control process with semantic understanding of content and deep-learning-driven risk analysis, so that data is protected based on thematic elements. In doing so, it hopes to make data access more fluid and less restrictive.

451 TAKE

We've written about data access governance (DAG) before. When done correctly, it can be an accelerator of worker productivity – ensuring the right people have access to the right data, at the right times, for the right reasons. However, simplistic rules-based or complex policy-based approaches most often require significant up-front planning to implement, and rarely are rule structures flexible enough to adapt to rapidly changing conditions. Inability to adapt can slow down the business, further frustrating well-intended workers who just want to get their jobs done.

Concentric is infusing DAG with a certain level of intelligence – using unsupervised deep learning to help cluster documents and other unstructured data types thematically, and calculating their relative risk. This approach understands that the protection of data depends on its content, themes and context more so than any specific predetermined rule. However, in a market with some DAG vendors touting capabilities across all data types, unstructured data specialist Concentric may have to work harder to underscore the value delivered via its differentiated IP.

Context

Concentric was started in 2018, with the three cofounders – Karthik Krishnan, Shankar Subramaniam and Madhu Shashanka – tracing their relevant lineage back to Niara Networks. When Niara was acquired by HPE in February 2017, Krishnan and Subramaniam took expanded roles in HPE's security portfolio, with Krishnan leading product management and Subramaniam in technical leadership roles. Shashanka, who has a doctorate in data science, left to run the data science and machine learning initiatives at Charles Schwab. The initial concept for Concentric was largely borne from repeated conversations with security professionals, and their feedback that security teams routinely struggled to adequately identify, account for, and protect high-value or high-sensitivity content.

Concentric came out of stealth in January, focused on unstructured data; however, the company started acquiring customers and implementing production deployments in 2019. The product was initially focused not on DAG, but more on the prerequisites and associated technological capabilities that are complementary to it. The initial focus and tiered set of offerings provided three modules: data discovery and classification, risk monitoring, and remediation. These remain core elements of the company's capabilities to date, and the DAG functionality announced in fall 2020 is interdependent with the existing data discovery/classification and risk monitoring capabilities.

The company has raised $7.5m in two cumulative seed rounds, with participation from investors such as Clear Ventures, Engineering Capital, Homebrew and Core Ventures Group. The most recent round was raised in March 2019.

Concentric is headquartered in San Jose, with a secondary operation dedicated to engineering based in Bangalore, India. The company currently has approximately 25 employees.

Technology

Concentric, as mentioned above, offers data discovery and classification, risk monitoring, and remediation capabilities as its core components. In this sense, the new DAG capabilities are not a stand-alone offering, but rather interdependent of and packaged with the discovery/classification and risk monitoring modules.

The DAG capabilities, much like the rest of Concentric's portfolio, are focused on unstructured data. But rather than using predefined rules to modulate user access to specific content, the company is focused on an automated, AI-enabled approach that observes existing conditions and semantic themes to group content based on similarity and score it based on relative risk, so that appropriate remediation actions and access permissions can be implemented. Using deep learning, the company's signature IP is its Risk Distance analysis, which essentially autonomously identifies access and activity risks in unstructured data.

At its most elemental, Risk Distance is a measure of how dissimilar the existing security practices are between a given document and similar documents. This analysis uses an unsupervised approach to look at a thematically similar cluster of content and compare its properties. Things such as who has access to the data currently, who it has been shared with, where it has been shared, and deviations or inconsistencies in usage are all considerations in the model.

From there, Concentric has the ability to automatically implement access controls for content in a number of ways, if the organization desires to do so. Whether the product fully automates this step, however, is entirely at the discretion of the enterprise IT team, which can decide to override or manually tune the DAG controls as seen fit for the organization.

Users of the Concentric product are served a risk-oriented dashboard UI with insight that has been autonomously derived via this technology. Groups of content can be thematically viewed (such as 'legal'), and Concentric's existing data discovery and classification tie in with the application of appropriate labels (such as NDAs), appending the content's metadata. Updated metadata can tie back into the organization's policy framework. For privacy use cases, discovery and classification are also useful for identifying and appropriately governing personally identifiable information access. The product, additionally, can integrate with existing metadata management investments and efforts.

Competition

Concentric's competition, for the purposes of this report, will be broken down into two categories with some inherent overlap: data access governance, and data discovery and classification. Not all data discovery and classification providers provide DAG, but they often integrate with and complement it.

On the DAG front, there is a laundry list of providers, although few actually specialize in unstructured data. Perhaps most significant in the context of unstructured data would be Varonis, which provides DAG as a complement to its data discovery and classification capabilities. Spirion is a significant provider in this space with discovery/classification capabilities for unstructured data, as well as granular protection and access options. Furthermore, any native capabilities for content access control in Microsoft will functionally compete, since Microsoft's productivity suite is ubiquitous and largely defined by document creation and management. A traditional content management provider like OpenText might also compete for mindshare, given Concentric's focus on unstructured data.

Informatica can administer access controls for data via its data-source-agnostic approach, although the company isn't an unstructured data specialist. The Okera Active Data Access platform leverages an embedded catalog to govern access to a broad array of data sources, including certain unstructured data types. PlainID leveraged policy-based (as opposed to role-based) access controls to help administer rights to data. STEALTHbits is well known for DAG capabilities, and in a move that bolsters DAG utility, has also increasingly gotten deeper into broad data privacy functionality. Other DAG providers include Broadcom, Cloudera, Cyral, IBM, Immuta, Micro Focus, Netwrix, Privacera, SailPoint, Satori Cyber and Saviynt.

Data discovery and classification providers include the likes of IBM and Privacera, both of which also happen to overlap via their DAG capabilities – although, again, they are predominately focused on structured rather than unstructured data. Other data discovery and classification providers include 1touch.io, BigID, DataGrail, HelpSystems (via Bolden James and TITUS acquisitions), Infosys, Io-Tahoe, NetApp (via Cognigo assets), OneTrust (via Integris Software assets) and PKWARE.

SWOT Analysis

STRENGTHS

Concentric's IP is its Risk Distance capability, providing a technological differentiator in how it conducts assessment of risk and application of access controls. Using a semantic and automated approach, the company's technology relieves organizations of much of the up-front work required with traditional rules-based approaches to governing access to unstructured content. DAG capabilities are paired with data discovery and classification, increasing utility.

WEAKNESSES

Concentric has honed its DAG capabilities on unstructured data and does not currently have structured data capabilities, but it plans to expand in this direction. Some other DAG vendors are happy to tout capabilities that span all data types, although this claim should be taken with a grain of salt. Still, unstructured data represents only one piece of the enterprise data risk puzzle, albeit a very large and significant one. The company is quite small relative to many competitors in the space.

OPPORTUNITIES

The expansion of remote work has underscored the essential role that unstructured data plays in the lives of workers. Friction in data access is increasingly not tolerated, meaning rules-based DAG may need to be overhauled. With increased investment in collaboration and productivity technology, organizations might also be open to investing in DAG, which complements (and helps secure) productivity suites.

THREATS

While Concentric's existing risk analysis capability is a logical core component of its DAG, some potential customers might balk at packaging that necessitates use of Concentric's data discovery and classification capabilities. Many organizations already have existing investments in data discovery and classification, and might prefer to go with a vendor they already have a relationship with.