

REPORT REPRINT

BigID's big idea: A new app framework for data privacy and insight extensibility

JUNE 26 2020

By Paige Bartley

Enterprise data privacy efforts often begin with discovering, mapping and determining associated identity for sensitive data, but data privacy efforts often become siloed within departments. BigID's App Development Framework adds extensibility, exposing data intelligence via APIs so users of other IT tools can leverage data discovery and classification context.

THIS REPORT, LICENSED TO BIGID, DEVELOPED AND AS PROVIDED BY 451 RESEARCH, LLC, WAS PUBLISHED AS PART OF OUR SYNDICATED MARKET INSIGHT SUBSCRIPTION SERVICE. IT SHALL BE OWNED IN ITS ENTIRETY BY 451 RESEARCH, LLC. 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 451 RESEARCH.



Now a Part of

S&P Global Market Intelligence

Data privacy efforts require multiple stakeholders, ranging from compliance and legal all the way to IT and security, and the dedicated privacy practitioner community, too, is growing. The task of executing a single data subject access request (DSAR) – only one of countless regulatory requirements – could easily span multiple departments in a large organization. Furthermore, data privacy practices need to be embedded in other processes, such as development and testing. For the enterprise, all these personas often have preferred tools and workflows.

As data privacy programs operationalize, they need to extend their reach to other business functions. For example, according to 451 Research's Voice of the Enterprise, DevOps, 2H 2019 survey, 29% of respondents reported that 'concerns about governance, security and compliance risks' were a primary barrier to deploying DevOps for their organization. Lack of an integrative approach can slow everyone down. What BigID is aiming to do with its App Development Framework, introduced in June 2020, is to create extensibility and weave together this ecosystem of preferred tools so data privacy intelligence and context can be systematically surfaced throughout the organization.

451 TAKE

The concept of an app ecosystem isn't new, but as data privacy programs mature, there is pressure to expand privacy functionality and insight to existing IT investments. Traditionally, data privacy tools and platforms have focused on individual integrations, primarily to gain visibility into data repositories and sources, such as databases and SaaS apps. However, bidirectional relationships were less common; data privacy platforms tended to be 'home base' for privacy policies and context, with that context less likely to be visible or integrated into other common end-user environments.

BigID's App Development Framework is the scaffolding for extensibility of BigID's core competencies – finding, inventorying, classifying and mapping of data – which represent the far-left-hand side of the data privacy workflow. Apps have the potential to embed data privacy context into complementing IT systems, and the app model makes it simpler for organizations to make incremental investments in privacy. The challenge for BigID will be to gain critical mass with app development and community engagement, with the need to maximize the network effect so apps proliferate.

Context

Over the last two years, BigID has grown at a clip, with an initial inflection point in visibility and VC attention occurring when the company won the RSA Conference's Innovation Sandbox contest in 2018. When we wrote about BigID in the fall of 2019, the firm had just landed a \$50m series C round led by Bessemer Venture Partners. Since then, BigID has doubled down with another series C round of \$50m led by Tiger Global, announced in January 2020, bringing total funding to \$146.1m.

The company was founded in 2016 by the CEO Dimitri Sirota and chief product officer Nimrod Vax. Both were CA Technologies veterans. Within two years, by late 2017, BigID had begun to generate revenue. The company was founded jointly in Israel and the US, and currently its headquarters are split equally between Tel Aviv and New York.

Today, BigID has hit the 200-employee mark, and is still growing despite the global economic circumstances caused by the coronavirus pandemic. When we last wrote about BigID in March 2019, the company had approximately 90 employees – effectively doubling in headcount over the last year. Currently, BigID has about 70 customers, primarily enterprise, up from 35 in the spring of 2019.

The company's flagship platform, BigID Data Intelligence Platform, is where its foundational data privacy capabilities reside. The platform is enabled by four core pillars of functionality that power the company's signature data discovery: data catalog, data classification, cluster analysis, and correlation.

To discover data across the enterprise, however, requires data access. BigID facilitates this via 100+ agentless native connectors for a multitude of data types and architectures. The platform can handle data on-premises or in the cloud, structured and unstructured data sources, and data both at-rest and in-motion. Existing native BigID applications sitting on top of the platform architecture address various use cases under the umbrellas of data privacy, data protection, and data 'perspective' or insight.

Strategy

Today more than ever, organizations are looking to maximize the value of existing IT investments. According to our Voice of the Enterprise: Digital Pulse, Coronavirus Flash Survey June 2020, two-thirds (66%) of organizations are experiencing, or have experienced, an increased strain on internal IT resources as a result of the COVID-19 crisis. While much of this strain applies to the infrastructure supporting remote work, it would not be unreasonable to assume that the IT function within the enterprise is generally under pressure – to first optimize existing tooling and platforms, before making net new purchases.

BigID's App Development Framework, and the accompanying BigExchange community, are seeking to provide the architecture and developer resources for applications to be created by other parties, which will subsequently be shared with BigID customers via a store-like app-shopping experience. The objective is to maximize the utility of the systems that apps are created for, such as data catalogs, so that BigID's data discovery intelligence can be surfaced directly within those products and consumed natively via the UI. Bidirectional design allows for a metadata feedback loop between products, so context can flow both ways – for instance, allowing policies to be created in one system, and executed in the other.

The app model is designed to provide organizations with flexibility and modularity, allowing them to extend their privacy, data governance and security programs in a step-wise fashion in accordance with their existing IT environment and usage patterns. A few community apps already exist, and there are currently 10 BigID-developed apps spanning use cases from consent governance, to breach investigation, to data quality. Partners currently account for most of the community apps, with examples such as Collibra and AWS Security Hub. One of the objectives of the BigExchange community is to have more apps developed by partners and customers.

Part of the challenge in creating an app ecosystem is developing a community and encouraging engagement. For this, BigID is initially targeting developers via its outreach, providing a community portal with resources, tools such as SDKs, and even social opportunities such as digital meetups. Pricing for the apps will depend on their origin. BigID native apps will be priced at a premium over the contract value for the platform, while partner- and customer-developed apps will have pricing determined on an ad hoc basis by the developing organization.

Competition

While an app development framework designed for participation by third parties is relatively novel in data privacy software, many other players in the PrivacyOps space (as defined by our Data Management Market Map 2019) layer their own native applications on top of core technology. Because BigID's partner app ecosystem is still relatively nascent, we will focus on its broader competition.

REPORT REPRINT

From a high-level perspective, BigID competes for mindshare with providers such as OneTrust and TrustArc, which also have native applications for functions such as consent management and DSARs. However, OneTrust is a BigID partner, and it and TrustArc compete primarily with BigID for budget in the first phase of privacy management implementation.

In the data discovery and classification space, numerous competitors also focus on privacy. 1touch.io is a discovery and classification upstart that caters to privacy use cases via its Inventa platform. Dataguise is an established player in this market that, over the last 18 months, has aggressively expanded into dedicated data privacy functionality and dashboards.

Many of the PrivacyOps providers we identified in late 2019 also start at the far left-hand side of data privacy workflow with sensitive data discovery and classification technology. By PrivacyOps' definition, these providers also offer expanded tooling to support and operationalize data privacy far beyond discovery and classification. Examples include Datagrail, Integris Software, Io-Tahoe, NetApp (via Cognigo acquisition), Privacera and Securiti.ai.

A few other firms play more generally in the PrivacyOps segment. 2B Advice is a European company that offers a multipurpose data privacy platform, in addition to privacy consulting and training. Ardent Privacy is a small upstart focused on implementing privacy controls at the data layer, aimed at data minimization.

Some of the large data management providers collectively offer data discovery and classification functionality within their portfolios, supplemented by broad data privacy support. Examples would include IBM with its Guardium line, as well as multiple capabilities within the Cloud Pak for Data. Informatica's Data Privacy Management (formerly Secure@Source) has numerous privacy-supporting capabilities, and integrates directly with the company's Axon Governance. Varonis is a frequent incumbent when requirements include structured, unstructured and cloud data.

SWOT Analysis

STRENGTHS

BigID's App Framework potentially enables customers to build an integrated data discovery and privacy platform via apps tailored to their existing IT environment, rather than having to go all-in on large purchases of product bundles. The approach, and pricing, facilitates additional ROI from existing IT investments.

WEAKNESSES

For now, the supporting App Development Framework is established, but the number of generally available apps is still nascent. There is obviously ample room for growth here, but BigID will need to aggressively target developers and partners, as well as select apps to prioritize for development based both on market trends and customer demand.

OPPORTUNITIES

The challenge of data privacy is that it needs to be integrated into every data-centric business function. The App Development Framework expands integration with existing IT investments so organizations can tackle privacy without abandoning preferred tools or workflows. This will be appealing today as organizations look to operationalize their privacy programs while minimizing spend.

THREATS

In introducing such extensibility of the platform, BigID faces the challenge of making a broader swath of enterprise stakeholders aware of benefits – the DevOps function, for instance, would need to know BigID has an app for a particular DevOps tool. The bigger threat is simply inability to gain critical mass with the number of apps developed. As partners expand their own offerings, the app ecosystem might be construed as competitive.