REPORT REPRINT

Integris Software leverages automation for continuous data privacy compliance

MARCH 11 2019

By Paige Bartley

Data privacy and data protection regulations are increasingly complex and difficult to manage. Integris takes a highly automated and machine-learning-driven approach for defensible implementation of policy for data, both structured and unstructured, at enterprise scale.

Summary

The EU's General Data Protection Regulation (GDPR) brought data privacy and data protection to the forefront of enterprise concerns. As data privacy and data protection regulations around the world continue to proliferate, each with their own nuances and requirements, the enterprise is now struggling to identify and manage sensitive data at the elemental level, and struggling to create cohesive human processes to support the data management and control workflow. Given escalating volumes of structured and unstructured data, the need for automation is a given.

Data privacy tools currently available on the market typically focus on either the technical control of data, or the coordination of human processes. Often the 'missing link' is direct remediation of sensitive data once it is identified. Integris Software is betting on the use of automation to fill this gap, in an approach it calls 'data privacy automation.'

451 TAKE

The data privacy market is noisy, with vendors coming from diverse heritages: consulting, security, data management and process management. No single software can make an organization compliant with GDPR or similar regulations, so the enterprise typically employs several solutions. However, there is often a gap in tooling when multiple products are in place: the step of automatically enacting appropriate policy on sensitive or personal data once it has been identified. This is the layer of control that Integris is looking to implement, and it's a critical one for continuous, defensible compliance. The product's extensive use of automation and machine learning, for both detection of sensitive data and assignment/execution of policy, is necessary given escalating volumes of enterprise data that cannot be manually evaluated and assigned protective policies.

Context

Integris Software was founded in 2016 by current CEO Kristina Bergman, whose background in venture capital is significant. Her previous role as a principal at Ignition Partners led her to focus on evaluation of cloud, big data, security and IoT startups. In looking to found her own viable software company, she leveraged her existing knowledge of the market and its trends to identify potential gaps in functionality and capabilities. Data detection and data privacy, while addressed by many vendors in the ramp up to the GDPR deadline, often faced a gap in workflow and capabilities around assignment and automatic enforcement of data policies once sensitive data was found.

The company has about 25 employees, and is based in Seattle – its growth objective is to expand to at least 35 over Q2 2019. Currently venture-backed, Integris raised a $10m series A financing round in July 2018, led by Aspect Ventures with participation from Workday Ventures, Madrona Venture Group and Amplify Partners. The most recent funding round brings total funding to $13m. Madrona and Amplify led the initial seed rounds of funding.

Integris does not currently disclose the number of customers it has, although it reported 1,000% growth as a company between 2017 and 2018. Major regulatory mandates, such as GDPR and the California Consumer Privacy Act (CCPA) are currently its largest source of customer traction and interest; however, the company's long-range plans are to emphasize core capabilities and use cases outside of compliance.

Products

The Integris flagship platform is designed to help automatically detect sensitive and personal data, and importantly, automate remediation and policy execution once that data has been identified. The company deems this approach data privacy automation, and these capabilities ensure that data is automatically protected with appropriate measures once it has been identified.

The product's privacy policy manager capability supports over 250 sensitive data types out of the box – more can be added – and the enterprise can create policies and rules, add documentation, and exert granular policy control down to the column level. A DSAR (data subject access request) portal and dashboard helps manage requests for personal information from the public, allowing integration into ticketing systems such as ServiceNow or Jira.

The product's initial data discovery capabilities, which address the enterprise need to simply understand what sensitive data it has in its possession, is driven by a connector-based configuration. Connectors allow organizations to connect to practically any data source: structured, unstructured, in-motion or at-rest. Once connected to data sources, the discovery settings (driven by machine learning) can be tuned and adjusted for confidence levels and accuracy depending on the organization's appetite or willingness to accept false positives.

Integris operates at the data element level, rather than just the metadata level. This allows the enterprise to understand exactly what personal data is in the IT environment and data sets, rather than simply inferring sensitivity from metadata analysis. It takes an element-level approach rather than an identity-centric approach, because not all sensitive data can accurately be tied to a specific defined identity. Additionally, the product can detect sensitive data both in-motion and at rest – a differentiating characteristic among many of the competitors the company faces.

At a high level, what the Integris platform is trying to provide is a data privacy hub for multiple stakeholders: CIOs, CTOs, CDOs, CISOs and CPOs, as well as various lower-level practitioners. Tools for visibility into where sensitive data resides, and the ability to automate policy actions on that data, help ensure that data isn't just discovered and documented, but that an appropriate control workflow is kicked off as well.

Strategy

Integris, like many other vendors, is riding the wave of enterprise urgency driven by data privacy and data protection regulations such as GDPR and the CCPA. These immediate requirements are certainly driving traction in the market, and are a primary reason for purchases. However, Integris sees its underlying product capabilities as having more enduring and broader use cases. Privacy, according to Integris, is simply the 'tip of the spear.'

In the long run, Integris' capabilities can be leveraged as a data logic layer, so organizations can add and control any type of rule to any type of data, for any use case. While regulatory mandates are naturally a major part of the company's marketing strategy, education of the market is also a focus.

Partnerships will be strategically significant for the company, given the software's situation in the stack. Because it exerts controls directly on data, leveraging automation, it can act as a 'last mile' for more process-oriented privacy and governance tools that do not touch the data themselves.

Catalog and governance platforms, where policies are crafted by business users and data stewards, typically need an integrated technology partner to ensure that data policies are consistently and automatically enforced. Integris helps fill this role, and while the company does not currently disclose its specific existing partnerships, it does maintain a close relationship with prominent providers in the data governance market, increasing its access to potential customers.

Competition

Integris is increasingly encountering BigID in the sales cycle, although their approaches and architecture differ. BigID takes a very identity-centric approach, relying on associating sensitive data back to individual known or potentially unknown identities using algorithmic matching. Integris focuses on data at the element level rather than the identity level, not relying on the individual data element's association with an individual identity.

Cognigo could also be considered a competitor, with similar product objectives. It, too, is focused on detecting and remediating sensitive data within the enterprise for privacy purposes, and the company has a similarly strong emphasis on AI and automation for the identification, classification and handling of data at scale. It leverages agentless architecture with software installed on a single server within the enterprise.

Privacy management platforms offer some overlap in functionality. The most prominent of these would be OneTrust and TrustArc, although it is important to note that these products are largely sophisticated process coordination tools, designed for business users, that rely on technology integrations and partnerships to exert direct remediation controls on data. Integris specifically puts more emphasis on the direct remediation and control of data.

For the initial detection and identification of sensitive data within the IT ecosystem, players such as Dataguise and 1touch.io overlap in functionality. Large data governance and data management providers such as IBM and Informatica, additionally, offer collective suites of tools and products that could arguably compete with Integris in the sales cycle. Their incumbent status raises their visibility, but no single product or module in their portfolios is designed to address the exact layer of control that Integris is exerting.

SWOT Analysis

STRENGTHS

Integris is addressing a common 'missing link' in the data privacy workflow: automated remediation and control of sensitive data once it has been identified. Its capabilities around automation are critical, given modern enterprise volumes of data, both in-motion and at rest.

WEAKNESSES

The data privacy market is incredibly noisy, and visibility will continue to be a challenge for the company given larger competitors. Messaging, and value proposition – particularly around creation of the 'privacy automation' market segment – will need to be clearer to resonate.

OPPORTUNITIES

Integris clearly sees market opportunity for its product capabilities beyond immediate regulatory mandates and deadlines. By positioning itself as a 'data logic layer,' the company can demonstrate proactive use cases beyond gloom-and-doom checkbox requirements for compliance.

THREATS

The biggest threat is the greater funding and size of its competitors, which come from multiple market sectors. Everyone wants a piece of the privacy pie, and incumbent vendors have the marketing muscle to crowd out smaller specialty providers, even when their functionality is not on par.