Market Insight Report Reprint

Coverage Initiation: Keyavi Data looks to fortify security with 'self-protecting data'

September 17 2021

by Paige Bartley

Many traditional information security approaches rely on protecting the infrastructure, networks and endpoints where data can flow or exist. Leveraging an extensive array of IP, Keyavi has engineered protection for data that is essentially embedded in the data itself, allowing the data to self-protect wherever it may go.

451 Research

S&P Global
Market Intelligence

Introduction

Some established approaches to information security are, in part, roundabout efforts to protect data. However, with the rise of cloud architecture and sudden shift to remote-work models – among other factors – many approaches, such as securing the perimeter, have been weakened or made less practical. Based on 451 Research's Voice of the Enterprise: Information Security, Budgets & Outlook survey, data security is now being prioritized. When asked to indicate top strategic security objectives for 2021, 'implement or improve data security' was the second-most-cited response (31.6% of respondents) from a lengthy list, outranked only by the objective to improve organizational security awareness.

Keyavi Data is a data security specialist that believes content – such as files – can only be fully secure if individual pieces of data can essentially be programmed to recognize changing environments and dynamically apply policies accordingly in a 'self-protecting manner.' The company has invested significant intellectual property in the technology supporting these self-protecting mechanisms for data, and suggests that the product has wide applicability – ranging from data privacy use cases to ransomware mitigation.

THE 451 TAKE

Data can be a tricky thing to apply security controls to, which is why we have often defaulted to protecting the infrastructure, architecture and devices that surround it. That approach is arguably no longer viable. Data travels too freely, particularly in the cloud, to not have its own embedded protection mechanisms that can adapt to different environmental scenarios. This is exactly what Keyavi Data is setting out to do, giving organizations the ability to pre-program policies into their data that allow it to adapt protections regardless of where it may go. Like giving a traveler detailed regional guidebooks, security policies allow the data to 'act' accordingly in different situations.

Potential differentiation for Keyavi Data lies in its extensive portfolio of awarded, pending and under-consideration patents. For enterprise customers, the potential benefit is likely the ability to reduce the end-user friction often associated with traditional methods of securing content. The rationale stands that, with a finer-grained security policy attached directly to the data, there is much less of a need for blunt restrictions around entire networks, repositories or applications. To broaden its market, Keyavi Data will need to expand to structured data sources.

Context

Keyavi Data came out of stealth in March 2020, perhaps an inauspicious time given the sudden global economic impact brought on by the COVID-19 pandemic. However, it did not take long for certain sectors of enterprise technology to benefit from increased investment due to the radically new dynamics of widespread work-from-home business models. Information security technology was one such category. 451 Research surveys project that data security will see some of the highest budget spending within the information security category. Keyavi Data considers itself poised to capture this intended investment.

Its product took approximately 10 years to develop, with a heavy emphasis on the development of the intellectual property designed to dynamically enforce policies on data and content, regardless of where that data goes or what conditions it may exist in. Today, the company has 12 patents awarded, four patent applications pending and four patents under consideration.

Keyavi Data recently relocated its headquarters to Denver, but the company was originally founded in Las Vegas. The Keyavi Data team currently has about 40 employees, with an emphasis on engineering and development talent. Growth ambitions for the remainder of 2021 involve expanding the development and engineering team by approximately fourfold. In September, the company announced a reseller program agreement with RCI Technologies, catering (primarily) to both life sciences/biotech and government prospect accounts.

Funding to date has been primarily via a rolling seed round, with a series A close planned by the end of 2021. The company is actively pursuing additional institutional funding. Earlier this year, the company received multiple awards from the RSA Conference and the Black Hat Conference.

Technology

The Keyavi Data flagship offering is its eponymous self-protecting data platform, underpinned by a proprietary policy engine that allows for detailed enterprise adjustment of multiphasic, nested data controls. Via extensive IP, the company has engineered mechanisms for enterprise content, such as documents, to dynamically apply and adjust security controls such as access rights and permissions, contingent on environmental and contextual factors like geography/geofencing, individual users and data classification settings.

The Keyavi Data platform is API-driven and leverages multiple client-level solutions that can interact directly with data to achieve desired data control outcomes. The platform uses client technology, but that technology can be fully installed on the operating system of the device or in a browser mode, as well as in a web portal mode. All of these options provide full data security and control options for customers to use. Additionally, there is full Microsoft Office plug-in support (for applications such as Outlook, Excel, PowerPoint, etc.), and the Keyavi Data platform can be used to produce a plug-in for other common applications via its API system. The technology itself does not strictly require plug-ins to work, but plug-ins can (and do) improve the customer/user experience.

Critically, data protected by Keyavi Data is able to 'phone home' regardless of where it travels, reporting not only on its current protection status and settings, but also on the telemetry and IT details of the environment it has been introduced to. Offline access control is supported for controlled data types administered under the Keyavi Data platform. Offline capabilities, while perhaps not as immediately dynamic as online capabilities, are still meaningful. A 'default safe and closed' policy can be applied to data, including conditional time-window or geo-location allowances, to enable offline access for a limited period of time. While Keyavi Data is currently focused on protecting enterprise content, which often is the natural home for sensitive data such as personally identifiable information, there are plans to expand to multiple common structured data formats in the near future.

Strategy

The final detail noted above – the ability for individual pieces of content to collect and report details on external environments – is what provides the foundation for Keyavi Data's current go-to-market push into the anti-ransomware market. The criminal ransomware business model, in essence, exists in three phases – initially locking the data, exfiltrating the data and selling the stolen data to external parties for profit.

Keyavi Data, via its self-protecting controls for files and content, primarily disrupts the second and third steps of ransomware models, potentially rendering the criminal profitability of the ransomware 'business model' null. Keyavi Data primarily partners with other technology organizations to bolster defense against the first ransomware step of initially locking the data, which, from a criminal ransomware perspective, is relatively high on effort and complexity, but low on return. By interrupting the viability of the second and third steps, Keyavi Data is proposing that it can short-circuit the long-term profitability of ransomware models. As the Keyavi-protected content/data reports back on its current environment, the logic follows that any malicious actor would expose their own data ecosystem and IT environment by trying to ransom or transfer Keyavi Data-protected files. Ransoming the data – and selling the data to third parties – would theoretically expose the malicious actors involved, potentially rendering them vulnerable to law enforcement or even counterattacks.

Currently, the Keyavi Data offering is primarily targeted toward enterprise organizations seeking to coordinate a high-level data protection strategy. Channel sales are currently the focus, but the company is flexible, and implements a meaningful minority of direct enterprise sales as part of its ongoing strategy. However, this does not rule out a potential future business-to-consumer strategy in which the company could roll out a product targeted toward individual consumers. Currently, Keyavi Data is focused on a VAR strategy rather than reaching out via direct sales to the consumer market.

Competition

In the data security market, it is often useful to segment technology providers via the business objectives they are trying to help organizations achieve rather than the specific technical architecture or underpinnings. It is not uncommon for competitors in this space to use very different technical mechanisms to pursue similar business outcomes for their enterprise customers. Apples-to-apples comparisons are rare, especially since many vendors rely heavily on IP for differentiation.

The overarching objective that Keyavi Data is trying to achieve is dynamic protection of the data layer itself, where files and content can adapt policy controls contingent on environmental factors. This significantly overlaps the product into the existing digital rights management (DRM) market. Example competitors would include Vera, acquired by HelpSystems, which now integrates with HelpSystems' acquired TITUS data classification and content-control technology assets. Varonis remains an incumbent brand in the protection of enterprise content, although its architecture and IP is different from that of Keyavi Data. TripleBlind employs a cryptographic approach to secure data processing, but also borrows elements of DRM to protect data. Seclore and Virtru additionally use DRM or DRM-like technology to protect information.

Votiro is a file security provider that focuses on the detection and isolation of safe file content rather than simply scanning for potential threats. Sertainty is a privacy-oriented data security provider that has a philosophically similar approach to Keyavi Data – aiming to provide data with its own self-protecting mechanisms.

From a pure data security perspective, it might be worth highlighting providers such as ShardSecure, which employs microsharding techniques to essentially 'shred' data into highly distributed and encrypted pieces. Solix and Very Good Security are also notable in the data security space, with Solix specifically having some expertise around security of unstructured content.

The data access governance market, which we have detailed in the past, may have some nominal overlap here in trying to control appropriate access to enterprise content. Providers that have experience and expertise in the control of unstructured data include Concentric.ai, SPHERE Technology Solutions and Okera.

Large providers in the cloud market will naturally bundle products to achieve enterprise data security outcomes. Examples include the Microsoft Azure portfolio (including native content controls in Office 365), as well as IBM's Cloud Pak for Security.

SWOT Analysis

STRENGTHS

Keyavi Data leverages extensive IP to differentiate itself in a crowded information security market. Proprietary controls for data functionally allow the data or content itself to apply dynamic controls based on shifting environmental conditions. Keyavi Data's current efforts around malware have the potential to disrupt the criminal profitability of malware entirely, at least for Keyavi Data customers.

WEAKNESSES

Keyavi Data is a relatively small technology shop with modest institutional funding, and is extremely heavy on data and engineering talent. This isn't necessarily a detractor from a technology strategy perspective, but market mindshare is a reality that must be reckoned with. Regardless of how strong the product is technically, the company will likely need to elevate its visible presence in the market.

OPPORTUNITIES

Ransomware mitigation is an area of focus for Keyavi Data. The opportunity with ransomware risk reduction is that it applies to both the B2B and B2C markets. While Keyavi Data is currently much more focused on the enterprise market, the company likely has two major opportunities: the OEM market with its API platform, and with the consumer market if it can support the technology with adequate business partnerships and expanded customer support structure.

THREATS

The information security market has historically been fragmented and siloed to some extent. Heavy vendor emphasis on IP rather than open standards does not necessarily advance the cause for more interoperable and unified security efforts. Keyavi Data's relatively modest business footprint and funding trajectory may make it an attractive acquisition target, even if the motivation is simply to eliminate potential competition.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence