

**Publication date:**

29 Jan 2021

**Author:**

Tanner Johnson

Senior Analyst, IoT Cybersecurity

# On the Radar: Keyavi Data Corp. makes data intelligent, helping it to secure itself

# Table of Contents:

Summary .....	2
Market context .....	3
Product overview .....	3
Company information .....	4
Analyst comment .....	6
Appendix .....	6

# Summary

---

## Catalyst

Keyavi Data seeks to grant data intelligent, self-protecting, and self-awareness capabilities that ultimately help make the native security of the data itself more robust. This data security solution is provided through a comprehensive software-as-a-service/platform-as-a-service (SaaS/PaaS) application and through on-premises and white-labeled solutions that grant users extensive granular controls over each individual information asset. These individual controls can be altered and customized in numerous ways, granting or limiting access as needed, while allowing the data to report back on its own usage. Omdia refers to this emerging class of technology as *self-protecting data solutions*.

## Omdia view

In the age of regular reports about large-scale information breaches, it is apparent that traditional data security efforts often leave much to be desired. Despite a mature and growing cybersecurity market, data security solutions are frequently overlooked, ignored entirely, or completely mismanaged by a wide array of organizations. Despite these events, comprehensive defense-in-depth data protection remains a considerable investment, one that requires consistent digital due diligence to maintain it, because in the face of a breach, fundamental data protection efforts are truly the last line of defense for information security.

However, it is the great disparity in many organizational security practices that can introduce additional data protection hurdles. Many entities are struggling to deal with the impact of the global pandemic, changing compliance and policy demands, and the push toward digital transformation. As a result of the growing challenges that remain in place for information protection, Omdia projects that investment in data security solutions will see significant growth in the near term. The consistent demand for fluid data protection presents a welcoming market to vendors such as Keyavi.

## Why put Keyavi on your radar?

Keyavi's compelling self-protecting data offering provides customers with a comprehensive data protection solution that allows its users to exert granular managerial controls over individual files within their respective organizations. These include multilayered encryption, remote workforce enablement, seamless Microsoft Office plug-ins, digital rights management compliance, and a litany of other features. These protections are provided through the Keyavi platform, which grants each file the ability to report back to its respective administrator regarding its own behavior. The system also incorporates access control capabilities, because the platform enables customers to dictate the respective privileges of the users and alter them in real time. Additionally, customers can revoke another user's access to any asset, even after a Keyavi-protected file has been sent.

# Market context

---

Self-protecting data solutions will attract interest in the data security market, because they seek to provide users with greater operational insight into the overall activity of their corporate data. By allowing each data asset within an organization to report back to a command-and-control service for further instruction, self-protecting data solutions effectively endow data with its own intelligence. While the exact method these capabilities are provided with will likely vary between vendors, the overall result is a form of microcontainerization for data management.

In addition to providing greater granular security controls over data itself, these solutions help organizations meet frequently changing governance, risk, and compliance requirements. The fluid nature of policy development and compliance demands in enterprise environments dictates that comprehensive information management practices be followed and enforced. Self-protecting data solutions help to bolster these efforts by allowing protected data to truly audit itself with regard to which users have accessed (or attempted to access) specific files.

While the need for self-protecting data solutions is great, the market itself is still a nascent one. At the time of writing, Keyavi has begun to inhabit an emerging market shared with smaller, niche data security vendors. Past attempts at this include startups, privately held companies, and others such as Vera (HelpSystems) and Ionic Security. The Vera platform, acquired by HelpSystems in late 2020, is another data security solution but offers far fewer real-time data monitoring and protection features. The Ionic Security platform focuses on providing data control capabilities through its Machina policy-based authorization engine. At this juncture, Keyavi has no viable competitors.

# Product overview

---

As a result of the global pandemic, many organizations are struggling to regain control of the digital perimeters they once enjoyed via the physical office environments under their control. With the move to more online interactions and remote working motivated by precautions designed to stem the spread of COVID-19, that notion of *perimeter* was effectively shattered. The perimeter continues to expand and now must incorporate the individual home environments that form the foundation of a massive, virtualized workforce.

Therefore, in order for control of the perimeter to be regained, it must be able to move with the data itself. The Keyavi platform is a hybrid SaaS/PaaS, on-premises, and white-labeled application platform that aims to address this requirement by offering users a wide range of options for implementing their own self-protecting data security strategy. When deployed, Keyavi wraps files designated for protection within its own managed service perimeter. Information protection settings tied to the file's specific metadata are adjusted via the software suite interface.

Keyavi's solution—available as an API, client software product, mobile app, and a web client—offers a number of industry-first features, such as geofencing capabilities that allow the client to dictate from which locations a user is authorized to interact with any protected data. Another of the platform's design principles is the ease of the user interface, aiming to provide a seamless transition between home and

business network environments. Thus Keyavi works with any operating system or application, allowing for greater deployment and integration opportunities with legacy software configurations.

It is through these integration capabilities that Keyavi's platform allows real-time policy editing for files protected by the solution, allowing permissions to be revoked even after a file is shared. As the files also report back on their own behavior, they help provide a chain of custody that can greatly assist in compliance, reporting, and forensic audit requirements. The solution also offers advanced embedded protections for the various systems housing Keyavi-secured files.

To further facilitate the various functions of its self-protecting data platform, Keyavi has developed a custom API interface. The specific components of the platform include the client application, an administration portal, and a free viewer for all file recipients. There are also mobile clients for iOS and Android and plug-ins for email systems such as Microsoft Office Outlook.

# Company information

---

## Background

Headquartered in Las Vegas, US, Keyavi was founded in March 2020 by Elliot Lewis, the company's chief executive officer. Lewis has previously held executive security positions at Microsoft, Cisco, Merrill Lynch, and Dell. He is supported by five other members of the executive management team, with more than a century of leadership and security experience between them.

With 16 patents awarded and three patents currently pending, the organization continues to grow (along with demand for self-protecting data solutions). In addition, while Keyavi targets a wide range of verticals, including the ever-changing policy compliance environments of government and legal entities, healthcare and insurance, and even gaming and hospitality, there are few markets unsuited for deployment of the Keyavi's solution suite.

## Current position

While the company was born in March 2020, the organization operated in stealth for several years before reaching the critical mass that hastened an official product launch. The monetization of the self-protecting data solution is facilitated through a SaaS/PaaS licensing model, offered on a per user basis, with a minimum of 25 users required and volume discounts as the number of users increases. The company also offers licenses for its API integration and for OEMs to bolster their own secure product development.

The Keyavi self-protecting data solution has achieved FIPS-140-2 compliance with the National Institute of Standards and Technology (NIST) Security Requirements for Cryptographic Modules. While this compliance is required for the organization's traditional government and defense market clientele, market demand for greater data security requirements is likely to continue to evolve as the number of large-scale data breaches continues to rise and the disruption of traditional work environments persists.

## Future plans

Because it is a startup that is less than one year old at the time of writing, every decision made by Keyavi can be considered "future plans." The company's current go-to-market strategy, further orchestrated and

automated through its SaaS/PaaS platform, provides the simplest path for monetization and for incorporating updated features. However, while it is currently headquartered in Nevada and primarily focused on the North American market, Keyavi has plans to expand to other regions through established and new partnerships.

Any specific challenges and complications arising from expansion into other regional markets will likely stem from the need to remain as nimble as possible as a startup. In the face of ever-changing compliance standards surrounding data security, within a myriad disparate and evolving global policy requirements, Keyavi seeks to offer a product that can adapt to these changes swiftly for the individual nations operating within any global region. Furthermore, Keyavi recognizes the beyond, imbuing data with intelligence, self-protection, and self-awareness. The ultimate evolution of any self-protecting data solution would be to grant data a level of intelligence that would allow truly autonomous protection.

## Key facts

**Table 1: Data sheet: Keyavi Data Corp.**

<b>Product name</b>	Keyavi Data	<b>Product classification</b>	Existing: data security New: self-protecting data
<b>Version number</b>	10.0	<b>Release date</b>	March 24, 2020
<b>Industries covered</b>	All, with primary focus in government/defense, financial services, technology, manufacturing, legal/escrow, hospitality and gaming, cybersecurity	<b>Geographies covered</b>	US currently, with partner expansion globally
<b>Relevant company sizes</b>	All	<b>Licensing options</b>	Enterprise user licenses (25 minimum), API licensing, OEM licensing
<b>URL</b>	www.keyavidata.com	<b>Routes to market</b>	Direct, channel, OEM
<b>Company headquarters</b>	Las Vegas, Nevada, US	<b>Number of employees</b>	Not reported

Source: Omdia

# Analyst comment

---

Keyavi is a very young company and is entering a market with few real competitors sharing the niche space of intelligent data. This leaves a runway that is relatively clear for takeoff. However, one of Keyavi's main competitors, Vera, has been in the marketplace since 2014 and has recently been purchased by private equity firm HelpSystems. This acquisition further illustrates that vendors that have been in the area longer, even if only for a few years, pose a challenge for startups, which must now compete with larger entities.

The growing demand for data security offerings presented by these startups makes them ripe for acquisition by larger players looking to bolster their own portfolios. This route is often quicker and easier than investing in the development of a home-grown offering. Furthermore, with acquisition by a larger entity comes additional resources to promote the newly purchased service, effectively overshadowing the competition.

Self-protecting data solutions offered through data security vendors such as Keyavi are quite innovative. The ability to imbue individual files with the intelligence necessary to share real-time details regarding the respective file's own usage can help to distinguish these solutions from other security technologies that provide similar functions. For example, there are some authentication solutions that provide a few comparable capabilities that are more accurately classified as privileged access management solutions, which could potentially be modified to incorporate self-protecting data functions. However, the levels of granular control offered through self-protecting data solutions, as well as their integrations with legacy software, help to differentiate them in the market.

## Appendix

---

### On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

### Further reading

[\*Data Security Strategies Are at the Heart of Cybersecurity\*](#) (October 2020)

[\*Fundamentals of Zero Trust Access \(ZTA\)\*](#) (February 2020)

[\*"Data extortion: Ransomware with an evil new twist"\*](#) (February 2020)

### Author

Tanner Johnson, Principal Analyst, Data Security

[askananalyst@omdia.com](mailto:askananalyst@omdia.com)

## Citation policy

Request external citation and usage of Omdia research and data via [citations@omdia.com](mailto:citations@omdia.com).

## Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at [consulting@omdia.com](mailto:consulting@omdia.com).

## Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

## CONTACT US

[omdia.com](http://omdia.com)

[askananalyst@omdia.com](mailto:askananalyst@omdia.com)