

Self-Protecting Data Tech Overview

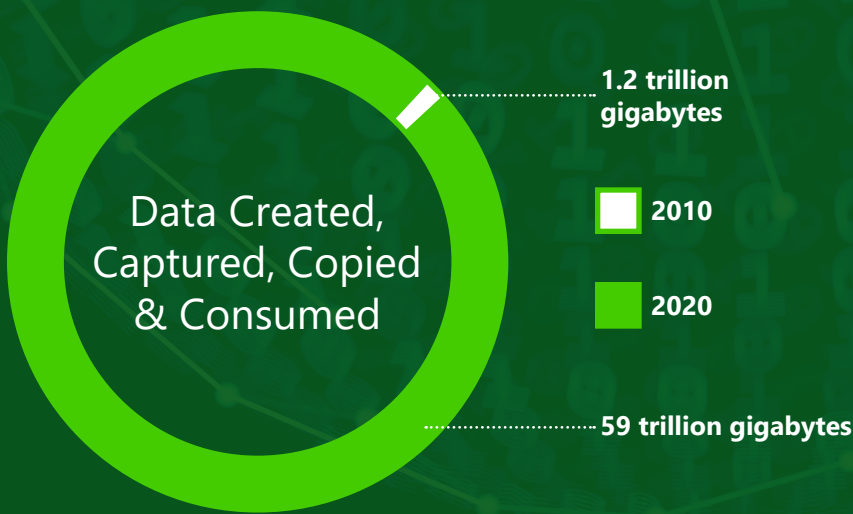
Ushering In the Era of Intelligent Data

The most valuable asset across all technologies and industries is data itself.

Most of today’s technology sets have failed to fully prevent data loss. At Keyavi, we believe the best approach to securing unstructured data is to infuse protection into each piece of data so that it can protect itself anywhere, anytime.

We have reached a critical juncture for securing sensitive data and protecting the rights and privacy of its owners. Keyavi has developed and launched an innovative solution that enables the security to travel with the data, making it self-protecting, intelligent and self-aware.

For most, having their data secured and truly protected at all times has been a far-reaching goal. Keyavi’s multi-patented technology gives data owners complete control over their data’s security, even after it leaves their possession. In this overview, we explain the need for a solution that can protect data at the source, how we designed it and how it works.

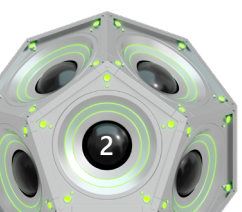


From 2010 to 2020, the amount of data created, captured, copied and consumed in the world increased from 1.2 trillion gigabytes to 59 trillion gigabytes, an almost 5,000% growth.

- Forbes -

The Dirty Little Secret in Cybersecurity

Until Keyavi, cybersecurity experts have mainly relied on data loss prevention and breach detection tools. Keyavi offers a new data security paradigm focused on enabling data to protect itself. Data, operating in the real world, is designed to flow and be shared as people and organizations constantly collaborate for business and personal transactions. What has been missing is the ability to **keep data absolutely protected** from the time it is created throughout its entire lifecycle by all intended recipients.



The Power of Infused Micropolicies

Simply treating the symptoms of data loss is one approach. At Keyavi, we believe that data protection should be infused into the data itself. Keyavi's technology provides many new advances for data protection in the real world:

Infuse protection into data itself. This is Keyavi's key differentiator that changes the fundamentals of data security. The owner can control access to the data by anyone, at anytime, anywhere it goes.

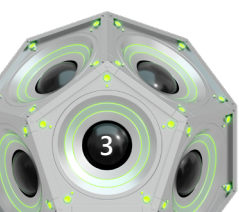
Install true intelligence and interactive decision-making into data itself. Static controls and rigid containment solutions have not worked because data, systems, devices, cloud and the internet are all too dynamic to be completely predictable. Data needs the ability to assess its security and adapt on the fly at all times, under any conditions and on demand.

Protect anywhere, anytime with agnostic control. Self-protecting data needs to work anywhere it goes, no matter the destination, platform, device, application, operating system, cloud service or data center. It must be universally deployable and interoperable to provide real-world protection across today's diverse environments.

Enable data to remove itself from a given situation on command by the owner. An owner has the ability to revoke access on demand, regardless of where the data resides. If the owner no longer wants the data accessible, the data has the ability to revoke or remove itself from access – long after it leaves its owner's possession.


Allow the data owner to maintain control throughout the data's lifecycle. Keyavi-infused data follows its owner's commands, policies and operational rules to remain safe even when the owner later changes permissions.

Provide forensic capabilities in logging and control, recording the data's complete experience throughout its lifecycle. This logging must be from creation and usage to storage and destruction. The data provides its own proof-of-possession, custody and control. It provides this information back to its owner on every copy that exists.




Making the Impossible Possible

Simplified, Keyavi has developed a proprietary multi-level “wrapper” system using patented multi-key encryption technology. The self-protecting data technology’s multiple encryption tiers achieve the following:




Protect and encrypt data content, either individual files or groups of files.

Cybersecurity has been based on one insurmountable, age-old premise – that data cannot protect itself. Now it can.



Create and apply policy and rulesets embedded into the “wrapper” of the data with more encryption, encompassing both the data and its encryption keys.



Define and deploy the policy sets, making the data accessible only under the right conditions: geolocation, identity of recipients, specified devices/services/platforms, time embargoes, digital rights management and more.

Our Platform: How We Made It Secure

Our wrapper technology is based on our patented multi-key system, which is designed so that no single key can allow access to the data. The layered key access model provides a systematic approach for data to evaluate its safety and situation without sacrificing performance:

The data can geosense and geofence. When data is outside approved locations, it can self-protect or stay encrypted and report back to the data owner.



The data assesses and approves its location and will confirm if rights have been revoked or changed, using industry-standard encryption controls.

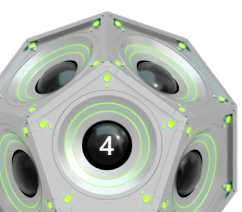


The data will unlock only if the recipient is still allowed access by confirming its policy models and intelligently processing its policy rulesets.



Finally, only when all other checkpoints are passed, will it then use another content key to allow access to the data.

If data is offline, a “default safe and closed” policy can be applied. Through conditional allowances, like geolocation and time parameters, Keyavi-secured data can be accessible offline.



Keyavi wraps and infuses the data with multiple independent encryption layers, so that no single layer can be compromised without triggering protection mechanisms in the surrounding layers. The data can only be accessed when all the owner's permission parameters are satisfied, which can be tailored to each owner's policy settings.

A data owner can allow or prevent access by geolocation, such as a company site and home office or at a street, state or country level. An owner can choose to change access permissions or revoke access completely from any or all recipients at any time – for the life of the data.

With the Keyavi API for enterprise customers and OEM partners, developers can build comprehensive data protection into their applications, products, firmware and services. The lightweight API allows developers to integrate data protection into existing applications and data workflows within the client, server, gateway or cloud.

Futureproofed and Built on Common Standards

Our architecture is specifically designed to be futureproofed for IT operations. Inevitably, cryptographic algorithm development and supporting technologies are constantly evolving and post-quantum cryptographic systems will likely emerge. Our technology is designed for use with any standard cryptographic APIs available on the underlying OS platform, device or platform where the data resides. We designed a "dual-stack" encryption model whereby the data can interchangeably use a public key infrastructure (PKI) to encrypt, decrypt and operate on all layers.

What Does Keyavi's Capabilities Mean for Existing Technologies?

Self-protecting data can be a game-changer in the world of cybersecurity. Keyavi works seamlessly to complement other cybersecurity solutions, eliminate redundancy and inefficiencies within your tech stack and dramatically enhance capabilities with all new data protection controls. This paradigm shift creates the foundation of a new technology ecosystem.

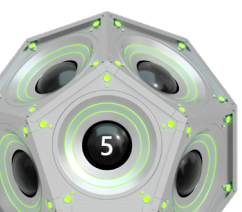
Obviously, security breaches will continue as long as attackers can successfully access valuable data. Regardless of other protections in place, when Keyavi's technology is infused into your data, that data will automatically know when unauthorized access is attempted and will protect itself.

When a file gets into the wrong hands, Keyavi's protection will prevent that valuable data from being exposed or extorted – making data breaches irrelevant. By making data self-aware, intelligent and self-protecting, Keyavi is putting the power and control back into the hands of the rightful data owner. This is a fundamental shift in data security.



Learn how Keyavi's self-protecting, intelligent and self-aware data security technology can boost productivity, growth and revenue.

[Learn More](#)





ABOUT KEYAVI

Headquartered in Durango, Colorado, Keyavi's self-protecting, intelligent and self-aware cybersecurity technology enables an individual piece of data to think for itself; secure itself; control where, when and who is allowed to access it; refuse access to unauthorized users; stay continually aware of its surroundings and automatically report back to its owner – with all these capabilities built into the data itself. The company's API platform and a full suite of applications riding on that platform also provide data owners with powerful controls to allow, revoke or deny access to their information – no matter who has it, on any platform or device, regardless of how many copies exist.

Under development for years before launching in 2020, this award-winning, multi-patented technology is so unique and innovative that leading industry analyst firm Omdia designated "self-protecting data solutions" as a new cybersecurity industry category, with Keyavi as the clear leader. Keyavi's easy-to-use yet robust solution delivers the ultimate in peace of mind for public and private organizations, their remote workforces and partner ecosystems in solving the security challenges of controlling confidential and intellectual property from data leaks, breaches and ransomware.

TO LEARN MORE ABOUT KEYAVI AND ITS BREAKTHROUGH TECHNOLOGY, VISIT [KEYAVI.COM/OUR-TECHNOLOGY](https://keyavi.com/our-technology).

FOLLOW KEYAVI ON [LINKEDIN](#), [FACEBOOK](#), [VIMEO](#) AND [TWITTER](#).

[KEYAVI.COM](https://keyavi.com)

DISCLAIMER

This publication is provided "AS IS" and all express or implied conditions, representations and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are disclaimed, except to the extent that such disclaimers are held to be legally invalid. Keyavi Data Corp. shall not be liable for incidental or consequential damages in connection with furnishing, performance, or use of this publication. The information contained herein is subject to change without notice.

No part of the contents of this document may be reproduced or transmitted in any form or by any means without the written permission of Keyavi Data Corp.

Copyright © 2022 Keyavi Data Corp. All rights reserved. Keyavi Data™ and Intelligent Directory™ are trademarks of Keyavi Data Corp. All other brand names, product names or trademarks belong to their respective owners.

