The common denominator and most valuable asset across all technologies and industries is data itself. Even the most advanced data containment solution sets have failed to fully prevent data loss. The answer is to infuse protection into each piece of data to protect itself, anywhere, always, throughout its lifecycle.

Data creation and exchange has profoundly changed the landscape of how each of us live, work and play. Data exchanges happen non-stop across the globe each day. Whether that data is being created by its owner or being shared and accessed by others, we have reached a critical juncture in the need to secure that data and protect the rights and privacy of its owners.

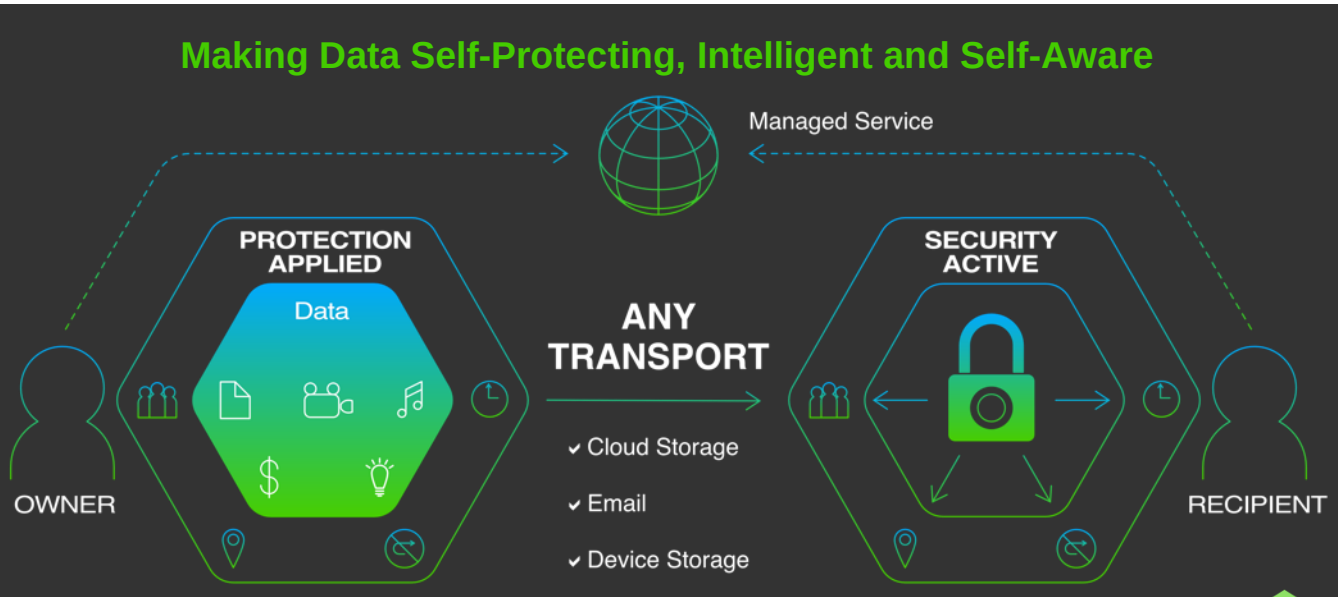
To that end, we at Keyavi Data have developed and launched our groundbreaking technology that makes data self-protecting, intelligent and self-aware.

Recognizably, many may be skeptical of these bold statements. For most, having their data secured and truly protected at all times has been an unattainable goal. But Keyavi's technology gives data owners complete control over their data's security – even after it leaves their possession. In this whitepaper, we explain the long over-due need for our technology, how we designed it and how it works.

The Dirty Little Secret in Cybersecurity

Until now, cybersecurity technologies have been limited by their technical capabilities and remain overly focused on data loss protection and breach detection in an attempt to contain data. But that is a losing battle: data – operating in the real world – is designed to flow and be shared as people and organizations are constantly collaborating for business and personal transactions. What has been missing is the ability to ***keep data absolutely protected*** from the time it is created, through its usage by all intended recipients, and throughout its entire lifecycle.

Control access to your data by anyone, anytime, anywhere it goes



Parameters for Making Data Intelligent

Simply treating the symptoms of data loss is wasted effort. Rather, the ***protection for data*** must be ***infused into the data itself***. Keyavi's technology provides many new advances for data protection in the real world:

- **Infuse protection into the data itself – fully contained with no external dependencies.** 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 on the fly, at all times, under any conditions, 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-word protection across today's diverse environments.

- **Enable the data to remove itself from a given situation at its owner's command.** The owner needs the ability to retrieve it or revoke access wherever it resides. If the owner no longer wants the data accessible, the data must have 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 its entire lifecycle.** Data has to follow its owner's commands, policies, and operational rules to remain safe even when the owner later changes permissions.

- **Provide forensic capabilities in its logging and control, recording the complete lifecycle of its experience.** This logging must be from creation through usage to storage to destruction. Data needs to be able to provide its own proof of possession, custody and control. It needs to provide this information back to its owner for every copy or instance from anywhere.

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.

- Create and apply policy and rulesets embedded into the "wrapper" of the data with more encryption – encompassing both the data and its encryption keys.

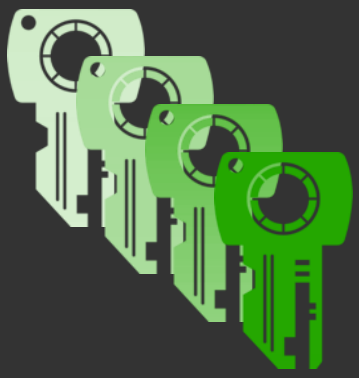
- Encrypt the policy sets, making the data accessible only under the right conditions of geo-location, identity of recipients, specified devices or services or platforms, time/day access embargos, digital rights management, and any additional policies the owner applies.

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:

1. The data is capable of geo-sensing and geo-fencing. If the data is outside its approved location set by policies, it will not allow any further interaction, with the option to self-delete to simply stay encrypted, all while reporting back to the data owner.
2. Using industry-standard encryption controls, if the data assesses and approves its location, it will then proceed to confirm whether the recipient's rights have been revoked or changed.
3. Using these same encryption controls, if the recipient is still allowed access, the data will unlock its policy models, and systematically process all of its rulesets to determine what it should do.
4. Finally, only when all other checkpoints are passed, will it then use another content key to allow access to the data.

If the data happens to be without connectivity, a "default safe and closed" policy can be applied including conditional time window or geolocation allowances.



Keyavi wraps and infuses the data with multiple independent encryption layers, so no single layer can be compromised without triggering protection mechanisms in the surrounding layers. The data can only be accessed when all of 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 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, wherever it is stored – by simply changing permissions from their device.

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 workflow within the client, server, gateway or cloud.

Futureproofed and Built on Common Standards

Our architecture is specifically designed to be futureproofed in operations. Inevitably, encryption controls will be upgraded, and new methods like blockchain and quantum encryption will take hold. Our technology is designed to use the CryptoAPI and controls on the device, platform, or OS that the data arrives on. We designed a "dual-stack" encryption model where the data can interchangeably use PKI and/or blockchain to encrypt, decrypt and operate on all layers.

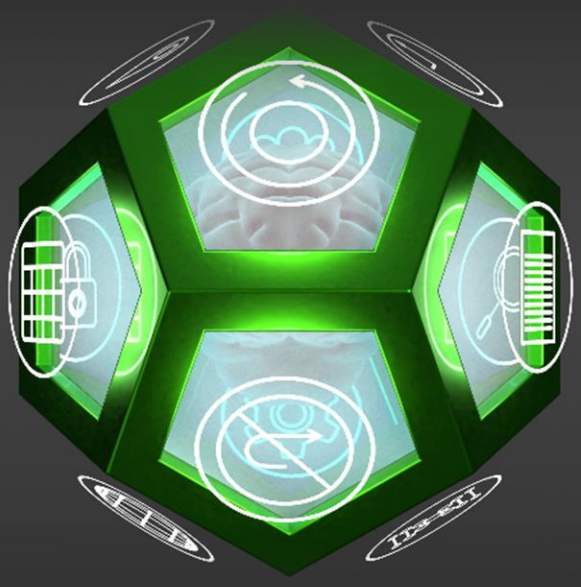
Keyavi does not access, store or intercept customer data in any way. The product is FIPS-140-2 certified and its forensic capabilities include possession, custody and control logging, as well as logging all access attempts (success and/or failure), creating a data "chain of custody" control for its owners.

TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments

What Does Keyavi's Capabilities Mean for Existing Technologies?

As with all truly evolutionary technology, this is a game-changer in the world of cybersecurity and technology. Keyavi works seamlessly to complement other cybersecurity solutions and dramatically enhance their capabilities with all new data protection controls. We believe this paradigm shift to be the foundation of a wholly new technology ecosystem.

Obviously, security breaches will continue as long as attackers are successful in accessing valuable data. But when Keyavi is infused into your data, regardless of other protections in place, your data will alert itself when access is attempted, and it will protect itself. Even if 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 changing the fundamentals of data security.



Now you can share data without ever losing control of it

About Keyavi Data

Based in Las Vegas, Nevada, Keyavi Data was launched in 2020 to eradicate data loss for enterprises in any market. Rather than trying to contain data in a world reliant on open information and transparency, Keyavi breaks new ground by making the data itself intelligent and self-aware, so that it can protect itself immediately, no matter where it is or who is attempting access. Keyavi's intelligent data platforms are compliant with FIPS-140-2 for NIST. Keyavi is led by a team of renowned experts in data security, encryption, enterprise software, and cyber forensics and analytics. The Keyavi name is inspired by the Italian word for key.